iGuard

IP-220E

IP/Network Camera

User's Manual

Version 2.5

CONTENTS

Chapter 1 Introduction

1.1 Features

iGuard-IP-220E is an affordable, versatile and flexible remote monitoring solution for small business, retail store, and residential applications. It can be accessed from anywhere in the world via a standard browser by entering the IP, account and password. Each system can simultaneously support any one combinations of USB PC cameras be it regular, infrared or pan-tilt. With its built-in web-server, iGuard-IP-220E can stream video images directly to the Internet without have to go through a computer.iGuard-IP-220E features a Windows-based software that allows the user to archive streaming video directly into the hard-drive. The same software also allows the user to monitor multiple cameras on one screen.

Features:

- Built-in USB port for additional camera expansion
- Support Pan/Tilt and Infrared USB PC Cameras
- Built-in Web Server
- 10/100Mbps Fast Ethernet Network Access
- Support Any Java-Enabled Web Browser
- 32-Bit RISC CPU
- 1MB Flash Memory
- 8MB Dynamic Memory
- Support Up to 30 Remote Viewers for each camera
- Allow Up to 8 User Accounts and Passwords
- 5.3VDC 1A Maximum
- Operating Temperature: 0°C ~ 60°C
- Operating Humidity: 10% ~ 90%
- Dimensions: 127.5mm x65.5mm x 58.5mm
- Weight: 331g
- Network Protocol: HTTP, TCP/IP, UDP, SMTP, PPPoE, Dynamic DNS, DNS Client, SNTP, BOOTP, DHCP, FTP, SNMP
- Support All USB PC Camera with VIMICRO ZC0301^{+} DSP processor
- Resolution: 640 x 480, 320 x 240, 160 x 120.
- Frame Rate: Up to 20fps in 320 x 240
- MJPEG compression
- USB 1.1 & 2.0 compliant
- Detailed Event Log with ability to sort and save

1.2 Function

The most important function of iGuard is for remote surveillance. Once iGuard is installed, the user can check any of the connected PC cameras via any web browser. The user can monitor and control these cameras simply by entering the IP address of the iGuard from anywhere in the world as long as there is an Internet connection. For instance, the user can be in Australia but he or she can monitor the production facility

in China, and if he or she likes, also check on the branch office in Singapore at the same time.

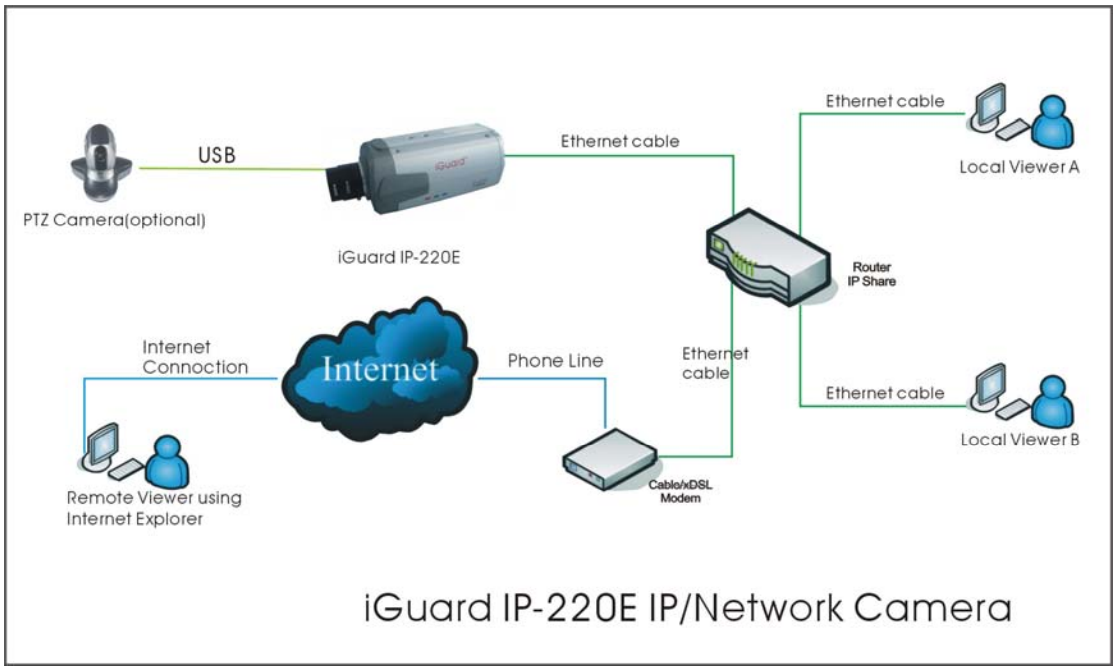


Fig.1 iGuard Network Diagram

1.3 Package Contents

Your iGuard package should contain the following items;

1. iGuard IP-220E Network Camera,
2. Ethernet Cable
3. iGuard Utility CD/Software
4. Quick Installation Guide
5. 5.3V DC Adapter

Chapter 2 iGuard IP-220E Hardware

Fig.2 iGuard IP-220E Camera

LED Status Indicators on iGuard		
Light color	**Signal definition**	**Condition description**
Green	Power state	On: Normal power
Red	Error Condition	On: Error condition occurred
Orange	Logon state	On: When there is user logon and receive the image.
Yellow	USB data activity	Flash when there is data transmit/receive on the USB.

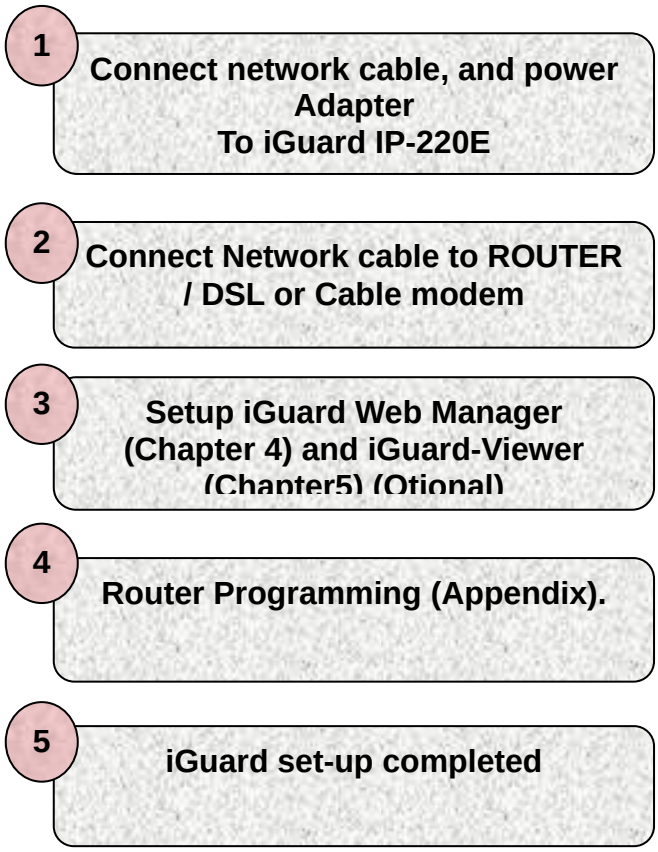
Table.1 iGuard Status LED Indicator

Light indicators on iGuard LAN Port LED	
Light color	**Condition description**
Green	On: Internet correspond speed is 100M Flash: Data transmitting/receiving
Yellow	On: Internet correspond speed is 10M Flash: Data transmitting/receiving

Table.2 iGuard LAN LED Indicators

Chapter 3 Hardware Installation

Before you start using the iGuard IP-220E network camera, you will need to set-up both the hardware and software. The following is a flow chart on the installation procedure:



3.1 Installation Procedure

Step 1:

Connect one end of the Ethernet cable to any available port on your hub, router, or cable/dsl modem.

Step 2:

Plug the other end of the Ethernet cable to the network port on the iGuard IP-220E.

Step 3:

Connect DC power adapter output into iGuard IP-220E socket.

Warning:

Please make sure the input Voltage and Frequency of the DC power adapter (DC 5.3V) is correct before plugging into the power outlet!

Chapter 4: iGuardware

iGuardware is a collection of two utility programs: iGuard Utility and iGuardview. You can use the iGuard Utility to quickly setup multiple iGuard units and you can use iGuardview to monitor multiple cameras, and maybe most importantly to perform motion tracking (V2.5 and above only). If you have a DHCP server on the network, the iGuard will obtain an IP address automatically, and you can enter this IP address in IE to launch the web manager (Chapter 5).

4.1 Installing iGuardware

Insert the software CD (or download from www.iguard.com) and click on setup if autorun does not start.

Fig.3 iGuardware Installation

- **iGuard Utility** - This is a program that helps the user perform quick installation. It will detect the current configuration and take the user through the necessary network setup.
  a. Click the 'iGuard Utility' button to start installation.
  b. After the step by step installation is completed, the iGuard Utility group will appear in Windows 'Start' ✳ 'Program Group'. "iGuard" Click this to start the program.

- **iGuardView** - This is a windows based program designed to allow user to control a large number of iGuard module located either in a LAN or on a WAN.
- **Read User's Manual** - Click to read iGuard's User Manual. You will need Adobe Acrobat Reader v5.0 or higher.

- **Adobe Acrobat Reader v5.0** - This will install Acrobat Reader v5.0 on your local hard drive.
- **Sun Java / ActiveX** - Install Sun Java for viewing the video image by Java, or install the OCX for viewing by ActiveX

4.2 Using iGuardware

4.2.1 iGuard Utility

The iGuard Utility main menu is shown below. The selection menu is located on the left. The Serial Number, current Firmware and IP Address of every iGuard connected to the LAN will be displayed on the table to the right.

Fig.4 iGuard Utility Main Menu

If the Devise Password is enabled at the factory, the IP address will be hidden and you will need to use the device password to launch the setup wizard, where you can reset the password.

If the password on your unit is disabled by your dealer and you are on the same LAN (same subnet) then you can use the web manager to configure the iGuard IP-220E camera by simply double click on the serial # of the camera. Everything discussed in this chapter can be repeated in Chap.5

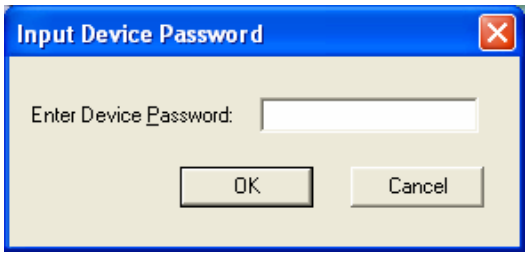
4.2.1.1 Setup Wizard

"Setup Wizard" will take you through the basic configurations step by step.

1. Click to highlight the iGuard on the right that you want to configure.

2. Click on "Setup Wizard".

   First, you must enter the device password located on the serial label to enter "Setup Wizard"; or "Launch iGuard", or "IP Configuration" if the iGuard has a preset password.



WARNING:
Do not lose this password. If the password is lost, you can not access the device to make changes. If you lose this password, you'll have to contact your reseller for the master password.

3. Once you have entered the necessary information for "Input Device Password" and "Administrator authentication", iGuard "Setup Wizard" will initiate to take you through the installation.

Fig.5 iGuard Setup Wizard

4. Enter the necessary camera configurations. Choose the appropriate frequency (Indoor 60 Hz, Indoor 50 Hz or Outdoor) to prevent flickering on the video feed. Enter a name for the camera in the “Location” box to easily identify it.

5. Click “Next >” to configure the Network Connection.

Fig.6 iGuard Network Setup

“Obtain an IP address by DHCP”

Choose this if you are installing the iGuard on a network with a DHCP server

“Use the following IP Address”

Enter an appropriate IP Address, Subnet Mask and Gateway for iGuard if have a static IP to assign to the iGuard

“Obtain an IP address by Bootp”

Allow iGuard to obtain an IP address using Bootp protocol.

6. Click “Next >” to proceed to xDSL/Cable modem setup.

   This section has to be configured to allow iGuard to access the Internet through an xDSL service provider.

Fig.7 iGuard a/DSL Setup

Select “Enable PPPoE connection” and enter your account and password details as provided by your internet service provider (“ISP”).

Otherwise, leave it at the default “Disable PPPoE connection”

7. Click “Next >” to change your administrator account and password information.

Fig.8 iGuard a/DSL Account Setup

An administrator account is necessary to ensure privacy. The user may revert to default settings, or if you do not set one, just delete the account and password and click “Next”.

WARNING: Do not lose the administrator account and password. Once set, you will not be able to configure iGuard without the administrator account and

password. To reset the iGuard account password, you will need to re-install the firmware using iGuard Utility.

8. Click “Next >” to upload these configuration to iGuard.

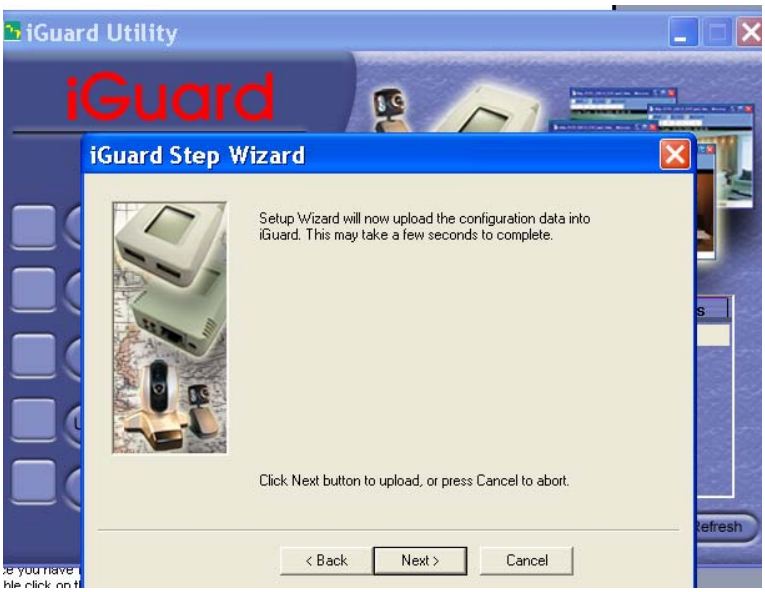


Fig.9 iGuard PPPoE Setup

9. Click “Next >” to save and restart iGuard with the new configurations.

4.2.1.2 Launch iGuard

Once you have finished with the above Setup Wizard, either click “Launch iGuard” or double click on the iGuard listed on the table, You will be bring to the iGuard Web

Manager(Chapter.5).

Fig.10 Launching iGuard

Key in the account name and password entered earlier (if you did not configure one, then revert to the default name “admin” and device password, OR just press ENTER or click on the “Apply” button, if the account name and password was not set and have been deleted).

Please refer to Chapter 5 for more details.

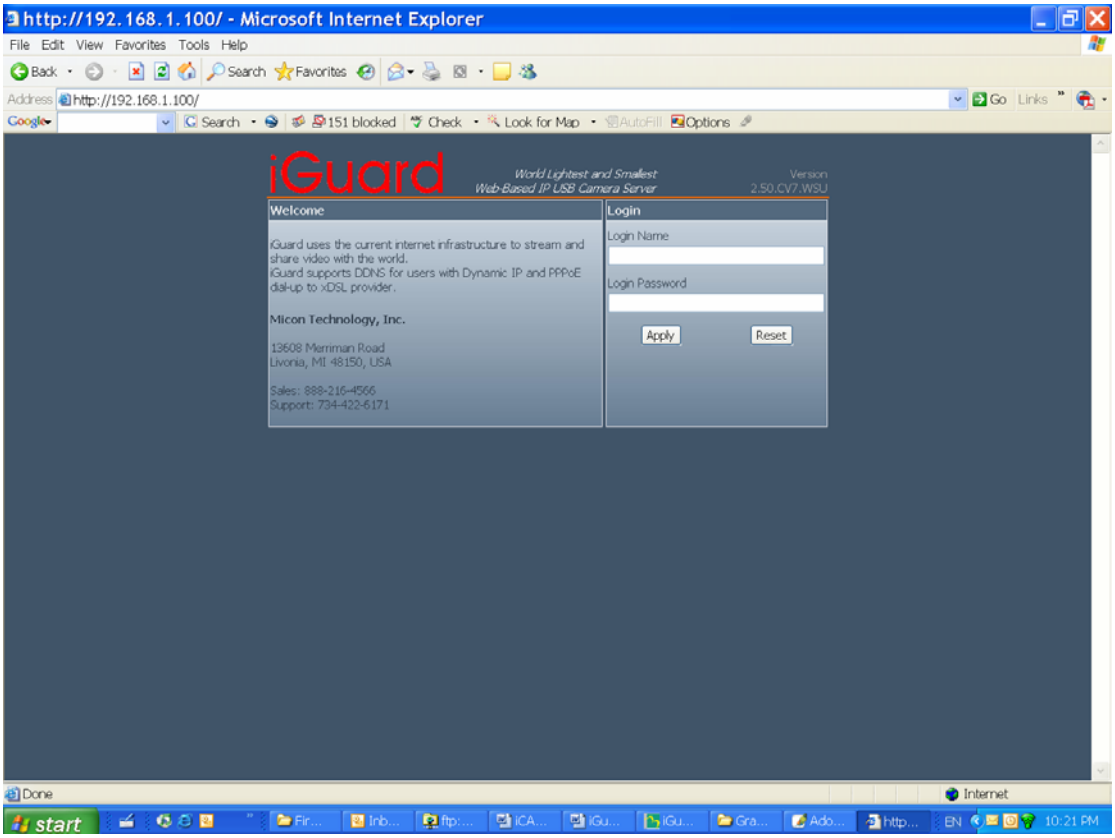


Fig.11 iGuard Web Manager

4.2.1.3 IP Configuration

This section allows you to set the IP configuration for iGuard.

Select the iGuard on the right display screen, and then click “IP Configuration”. This will bring up the IP Address Configuration window. There are two tabs;

- IP Address
- Advanced (for port setting configuration)

When using iGuard for the first time, it is advised to choose the “Using Static IP Address” option. For this option, the user will have to enter an IP Address, Subnet Mask and Gateway of their choice (refer to Appendix C for IP address explanation).

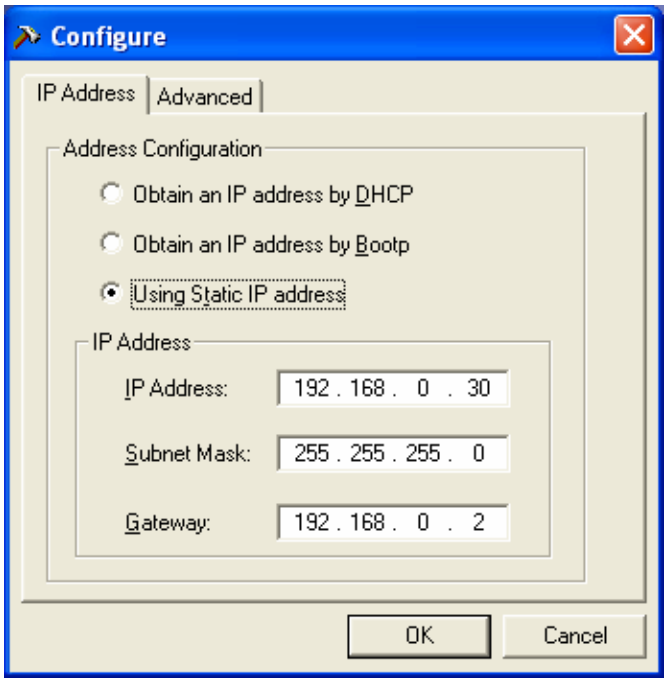


Fig.12 IP Configuration: Set an IP Address for iGuard

Once the IP Address is set, you will be able to connect to iGuard webpage by entering this IP Address into a standard browser.

"Obtain an IP address by DHCP or BOOTP"

The IP address, Subnet Mask and Gateway is acquired directly and assigned automatically by the system.

This "Advanced" section sets security password against unauthorised access to iGuard. Note, this password may be different than the administrator password.

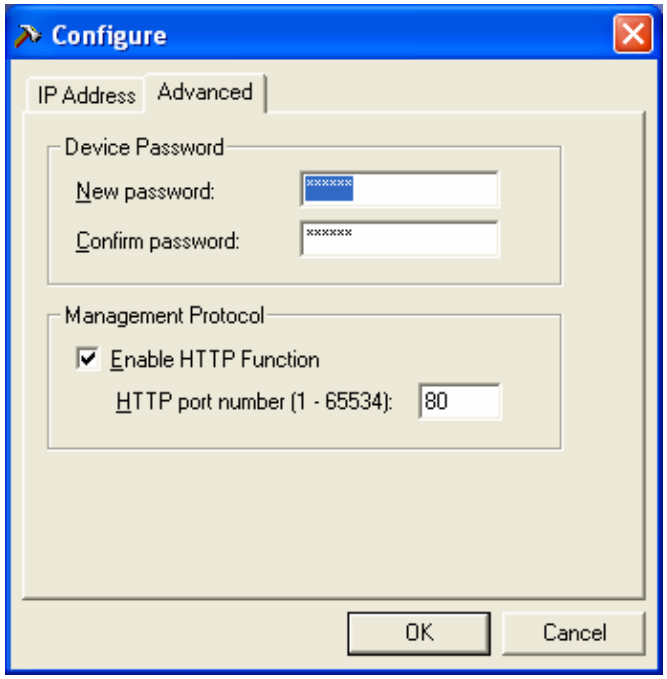


Fig.13 IP Configuration: iGuard Advanced settings

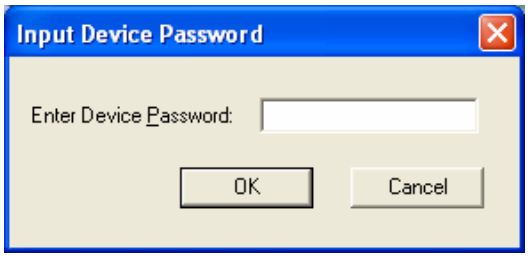
i. Device Password

Use this to set an access password to the individual device. Once set, the user must enter the password to access the device. In addition, the IP Address will not be shown on the right display panel of iGuard Utility.

Note: The default device password is set to be the same as administrator password, which is the printed on the serial label.

Fig.14 Reset Device Password

iGuard Utility will request for the “Input Device Password” when you click either “Setup Wizard”, “Launch iGuard” or “IP Configuration”



WARNING:
Do not lose this password. If the password is lost, you can not access the device to make changes. If you lose this password, you’ll have to contact your reseller for the master password.

To remove the password, you must first enter a valid “Input Device Password”, go to “Device Password” and delete the entries, click “OK”.

ii. Management Protocol

The administrator can determine the parameter settings when providing access via HTTP (web) to iGuard. For security reasons, the administrator can choose to use either an open or advanced port setting to control these access.

The default values are set to port number 80 for HTTP.

Once the HTTP port number is set to another port (other than 80), the full IP Address must be entered in order to access the Website.

For example:

- If a value of 61 is set as the HTTP port number, then http://192.168.0.177:61 must be entered as the web address in order to access iGuard website.

Uncheck to disable this function.

4.2.1.4 Upgrade Firmware

iGuard Utility offers a convenient method to upgrade iGuard firmware.

1. Click “Upgrade Firmware” to bring up the Wizard.

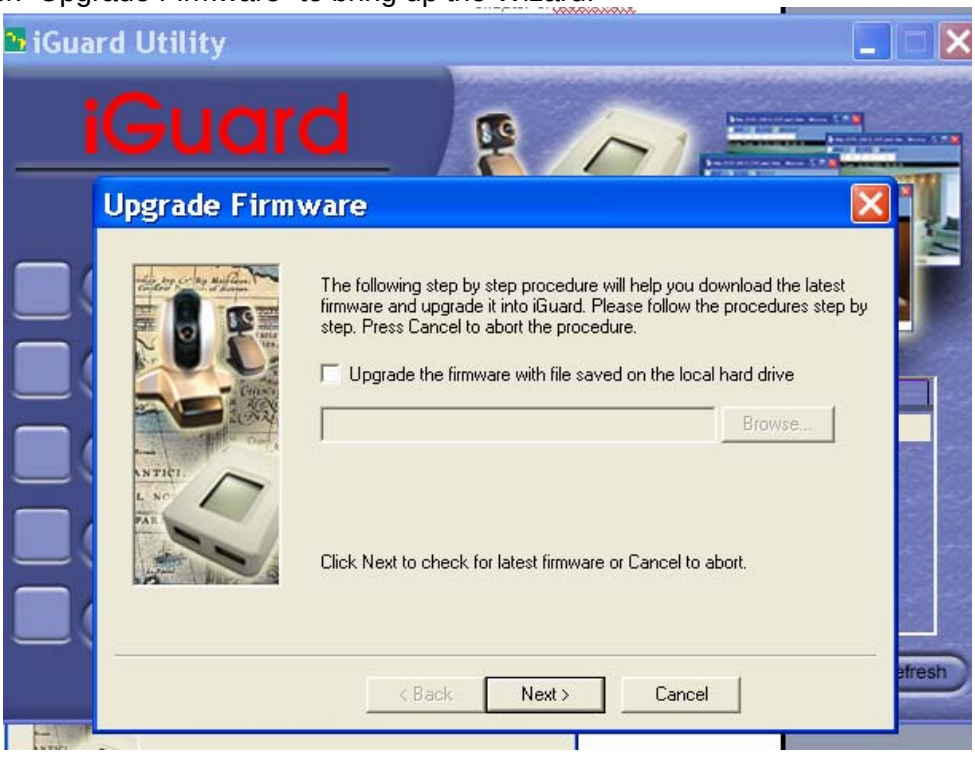


Fig.15 Upgrade Firmware: Updates iGuard firmware

If you have downloaded the latest firmware to your local hard drive, check “Upgrade the iGuard firmware with file saved on the local hard drive” and browse to the file location.

2. Click “Next >” to check for the latest available firmware.

3. Select new firmware file (*.bin) and,

4. Click “Start”.

The iGuard red and yellow LED will flash alternately to indicate that firmware upgrading is in progress. Once completed, iGuard will reboot.

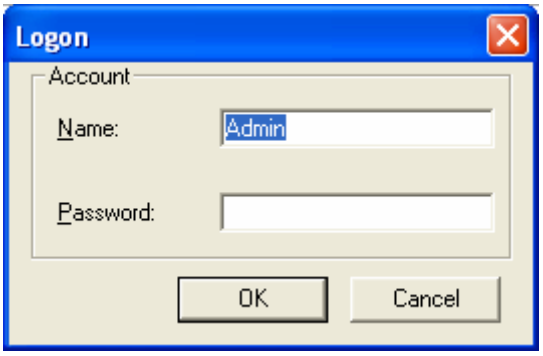
NOTE:
If the downloading / upgrade process is interrupted or the data is corrupted, the iGuard may become non-functional which is not covered by the standard warranty

4.2.2 iGuardView

iGuardView is a PC based utility software that allow you to manage and monitor multiple iGuard cameras located either in a LAN or on a WAN,

You can launch the iGuardView program by clicking on “start” - “Program” - “iGuard” - “iGuardView”

The following Login window will be displayed.



By default, the Account Name is set to “Admin” and No Password

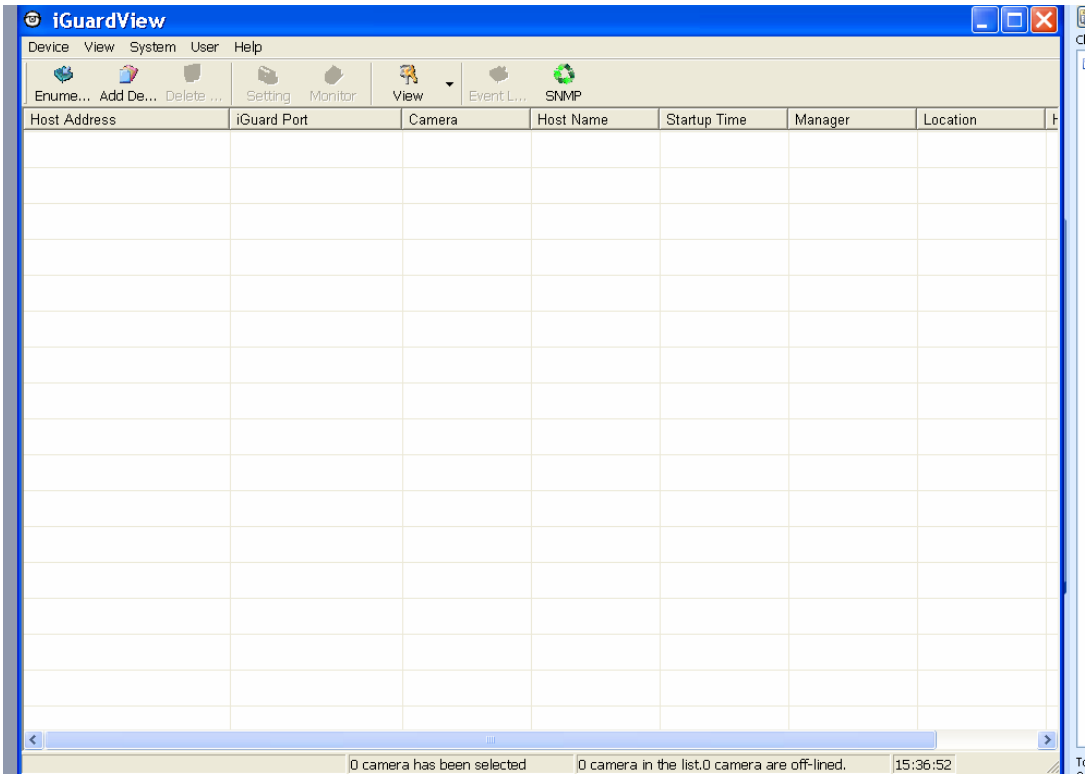


Fig.16 iGuardView Screen Shot

4.2.2.1 Device Setting

: Press the “Enumerate” button, iGuardView will start a search for all iGuard cameras under the same subnet and list them in the main window.

Once detected, the following will show in the main window:

Host Address	iCAMView Port	Camera	Host Name	Startup Time	Manager	Location
192.168.0.30	9001	Camera A				

This shows that the camera is online and active.

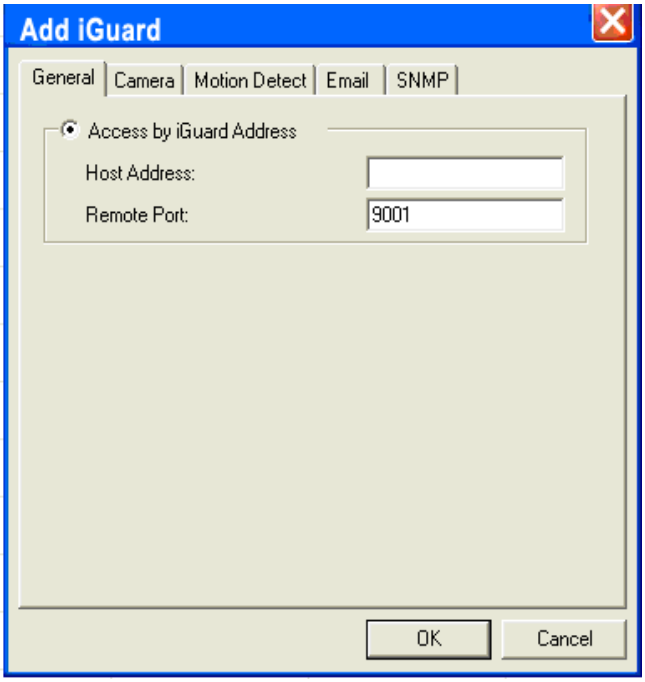
Host Address	iCAMView Port	Camera	Host Name	Startup Time	Manager	Location
192.168.0.30	9001	Camera A				

This shows that the camera is off-line

Manually adds the iGuard to be monitored.

“Access by iGuard Address”
Enter the IP address of the iGuard (example: 192.168.0.30)

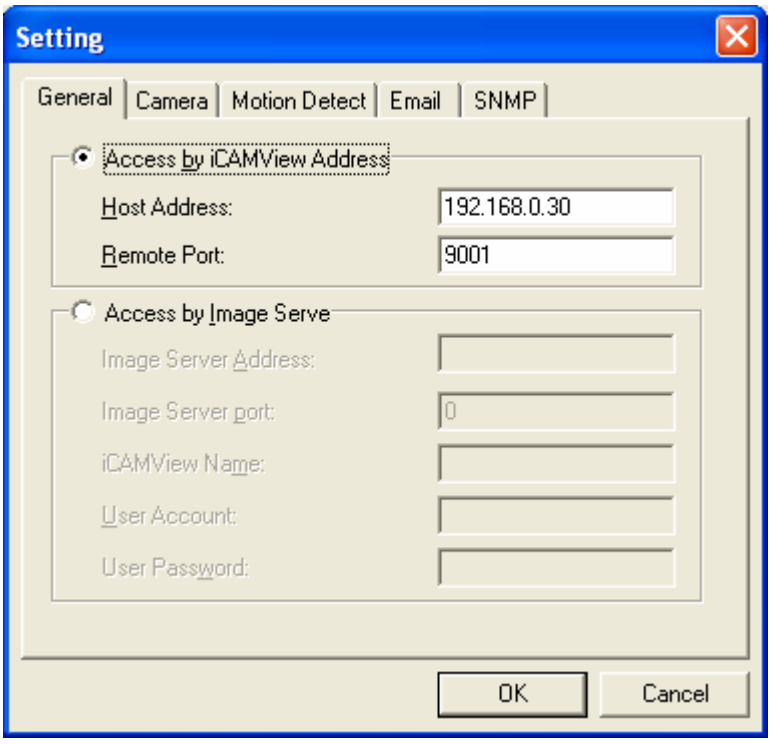
“Remote Port”
This is iGuard UDP port.



:

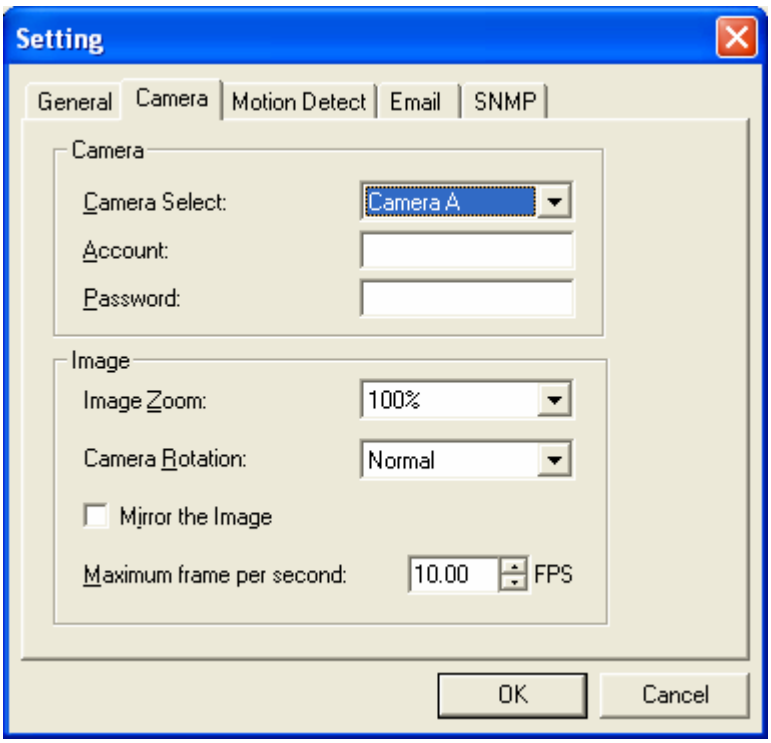
Highlight the iGuard to be deleted from iGuardView's list. Click "Yes" to confirm deletion of selected iGuard.

:



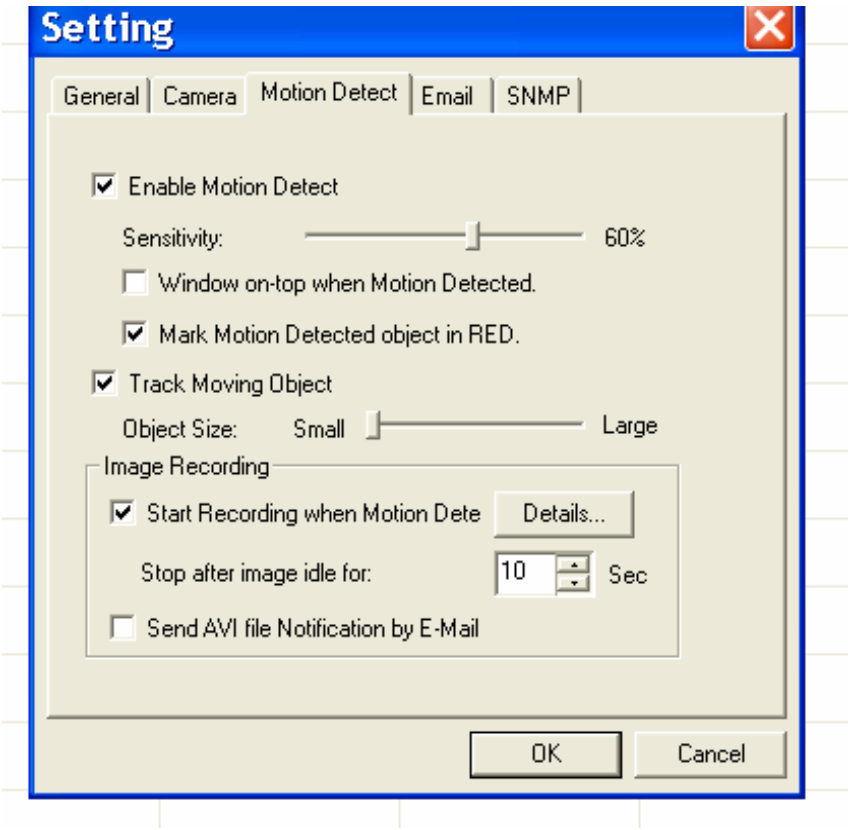
Use this function to change iGuard Address & Port Number.

4.2.2.2 Camera Setting



Camera Select:	Select either camera A or B
Account:	If you have setup user account, the information must be entered here. Otherwise access will be denied.
Password:	Enter the above account password.
Image Zoom:	Resize the window to between 25% and 200%
Camera Rotation:	Use this function to keep the camera up-right.
Mirror the Image:	To mirror the image.
Maximum frame per second:	Select from 0.01 fps to a maximum of 30.00 fps.
Time and Date	Check this to put Time and Date Stamp on Image

4.2.2.3 Motion Detection Setting



Enable Motion Detect	Click the checkbox to enable Motion Detection. **Note:** This feature requires the Camera Window be active to work. Click "Monitor" to activate the Window.
Sensitivity	Choose from 0% to 100% (very sensitive)
Window on-top when Motion Detected	Automatically displays camera window on top of all other windows/applications once motion is detected
Mark Motion Detected object in RED	Choose this option to highlight in RED which object is being tracked.
Track Moving Object	Choose this option to calibrate approximate size of object to be tracked
Image Recording	Click "Start Recording when Motion Detected" to enable the feature. Click the "Details.." button for the following options;

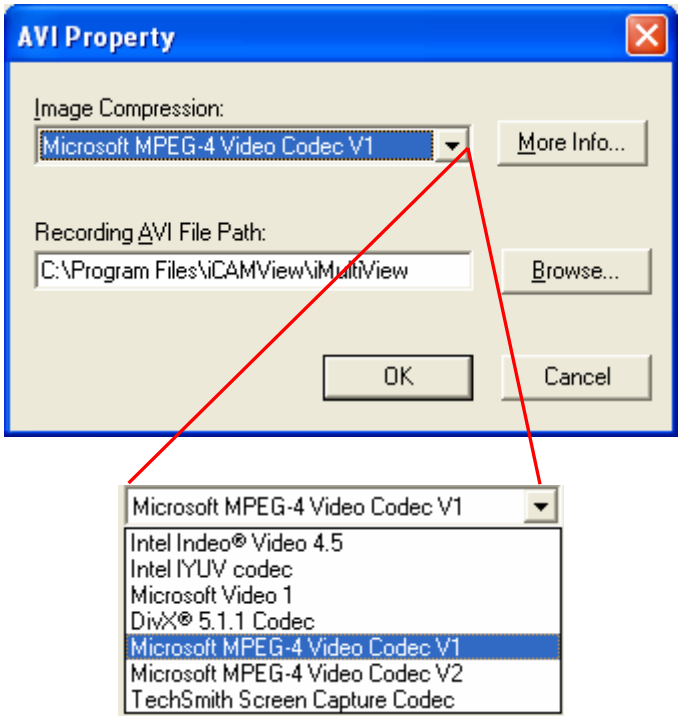


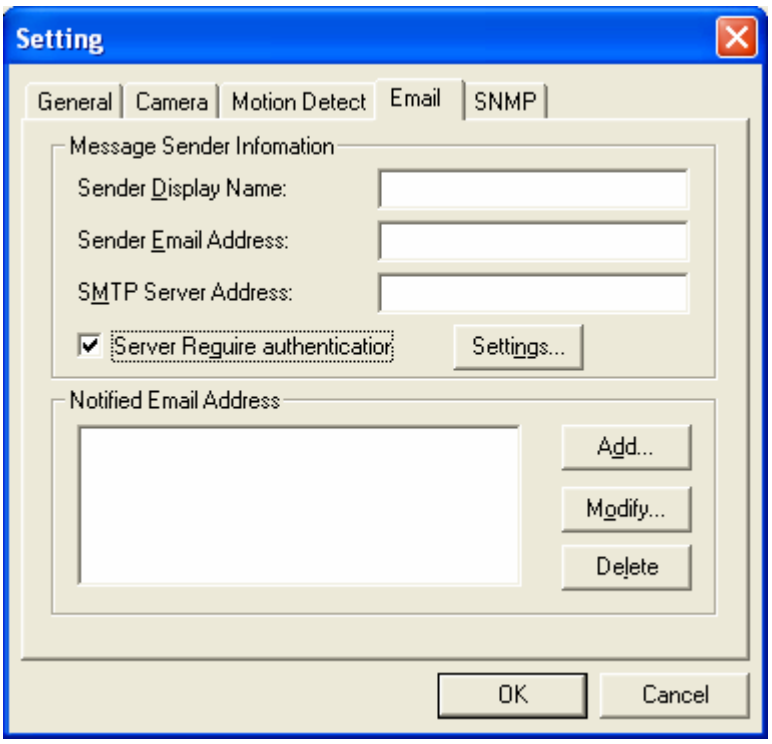
Image Compression:	Choose from the list of available compressions. **Note:** This list is dependent on the Codec that is available or already installed on the local PC. To record in MPEC-4, make sure you install or upgrade to Windows Media Player v10.
Recording AVI File Path	Location where the file will be recorded to. By default, it is recorded to C:\Program Files\iGuard\iGuardView. Click “Browse” to change the file location.

Recorded files are save using the following file extension;
avifile[three digit numerical sequence].

Note: Use the “Detail View” to check the record stop time. You can change the display view or add a new folder here.

Stop after idle for:	Set the value between 1 to 100 seconds
Send AVI file Notification by Email:	Send an AVI file via email in the event any motion is detected.

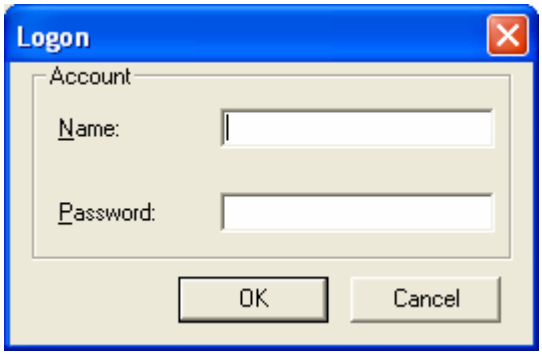
4.2.2.4 Email Notification Setting



You will need to configure the “Message Sender Information” in order for iGuard to send emails.

Server Authentication

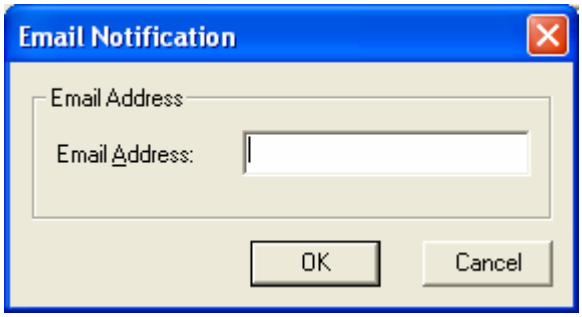
Click “settings…”



Enter your Account Name and Account Password if your Server Requires Authentication.

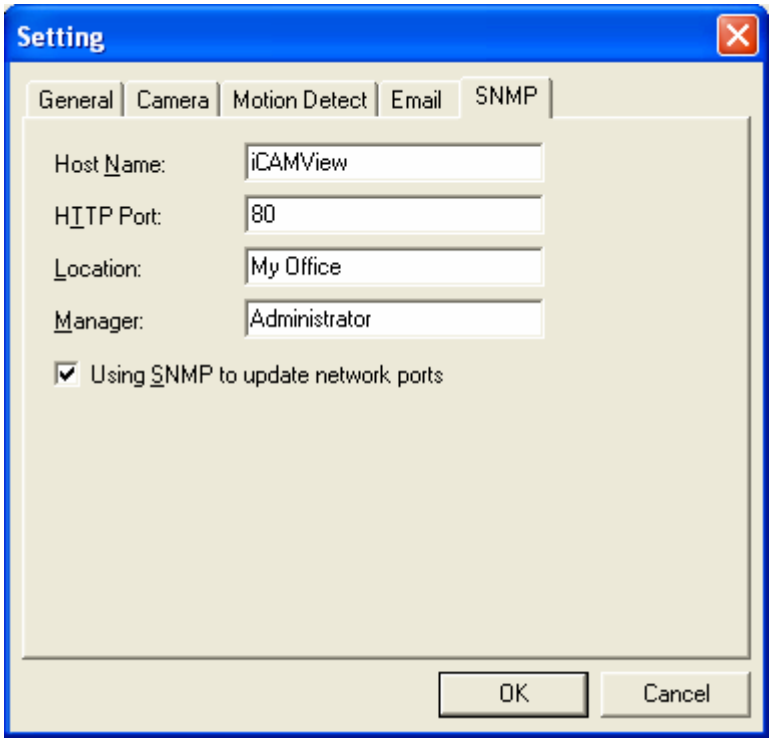
Email Address

Click “Add…” and enter a new Email address below



Click “Modify…” to modify the entered Email Address
Click “Delete” to remove an email address from the notification list.

4.2.2.5 SNMP Setting



Host Name: Provide a Name to identify this device.

HTTP Port: Enter the HTTP port assigned for iCAMView.

Location: Provide a location for SNMP manager to track device.

Manager: Enter a manager’s name for identification.

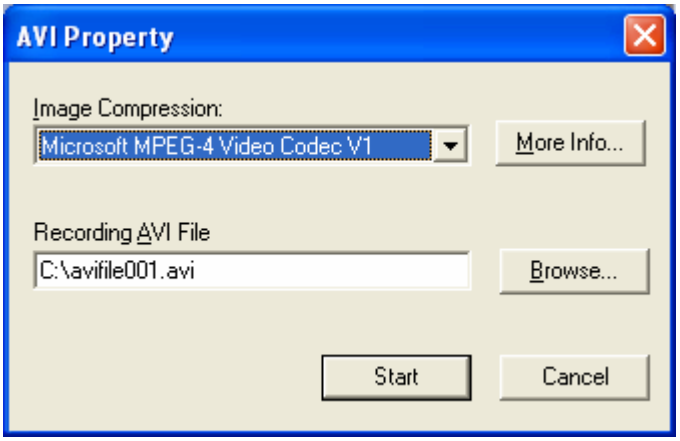
“**Using SNMP to update network ports**”
Check this box if you want iMultiView to automatically update the HTTP port as set in iCAMView Web (Basic settings✳Network✳Port Number✳Http port number) or iCAMView Utility (IP configuration✳Advanced✳Management Protocol)

4.2.2.6 Camera Monitor

: Highlight the iCAMView in the main windows display, and click "Monitor" to view the video stream.

Move the curser over the edges of the picture and it will turn into an arrow. Click and hold to pan / tilt the camera (if the camera supports this function)

Click this button to record the current image on screen. A window will come up, click "Start" to start recording to the default file and location.



Flip the image vertically

Rotate Left, Rotate Right

Click this to bring up the Setting windows.

Click this to switch to full screen view. Double click to switch back to current view.

Click and drag to resize the window and it's contents.

Date and Time display of live streaming video.

Click the left side of the viewing window to bring out more control features.

Click on this icon to active two functions;

a. Custom window zoom – use this to zoom to your chosen window size.

On the video window, **LEFT** click, hold and drag to the desired window zoom size. A thin line will outline the chosen window size.

Release to accept and the program will auto adjust. Increase the Resolution for a better image.

Click the depressed  button to go back to the original window size.

b. Custom update Window -- use this if you want to monitor only a specific area within the viewing window.

On the video window, **RIGHT** click, hold and drag to the desired window zoom size. A thin line will outline the chosen window size.

Release and a smaller window is shown. Video in this smaller window will be updated while those outside are 'frozen'.

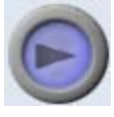
Click the depressed  button to go back to the original window size. Or use the horizontal zoom bar (see below).

Click and drag the green knob along the horizontal bar to zoom in an out. Zoom range from 1 time to 16 times.

Click and drag the green knob along the horizontal bar to change the current image resolution. Resolution range from 320x240 low/mid/high quality, to 640x480 low/mid/high quality.

Clicking once will cause the camera to pan left by 1 deg.

Click and hold and the camera will pan increasingly faster to the left.



Clicking once will cause the camera to pan right by 1 deg.

Click and hold and the camera will pan increasingly faster to the left.

Click once to tilt the camera up by 1 deg.

Click and hold and the camera will tilt increasingly faster upwards.

Click once to tilt the camera down by 1 deg.

Click and hold and the camera will tilt increasingly faster downwards.

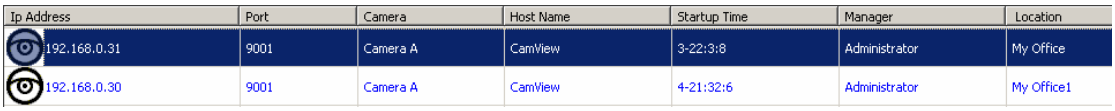
Auto Pan (if camera which support this function)

Note: The above Pan/Tilt button will only work with cameras supporting the Pan/Tilt function

4.2.2.7 View

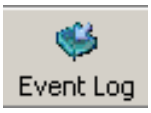
: Switch between Large or Small icon view

Large icon display

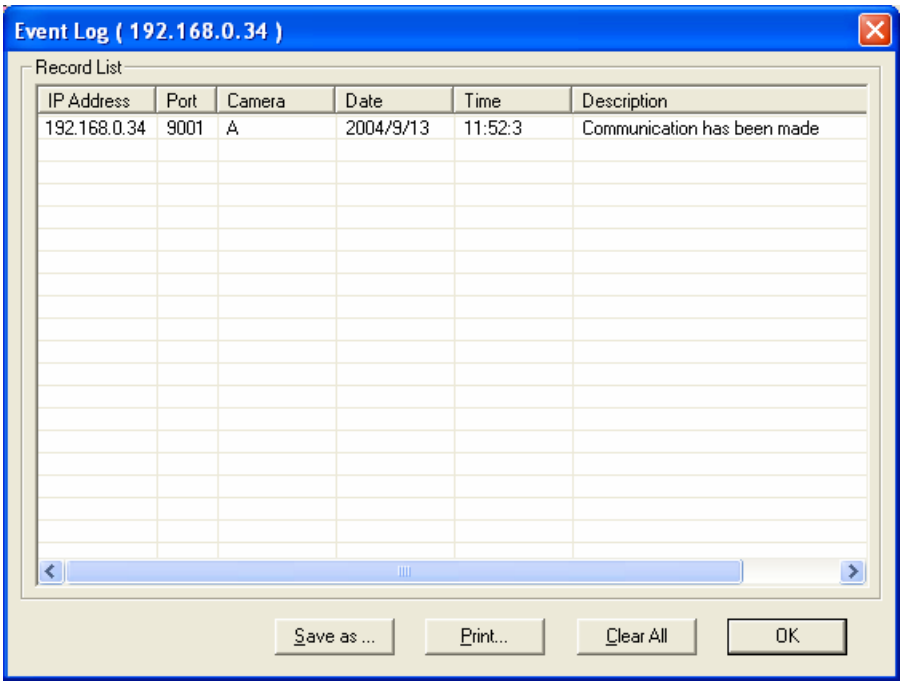


Small icon display

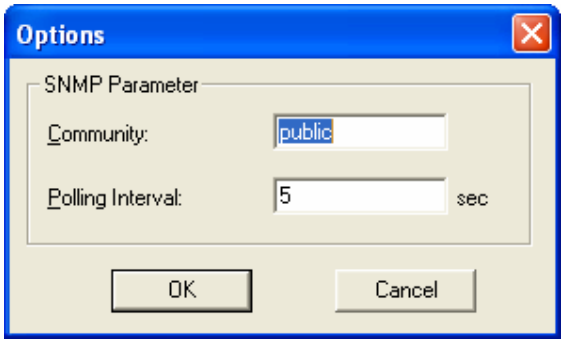
4.2.2.8 System



: Display the Event Log (IP address, Port, date, Time, description of event) of the selected iGuard.

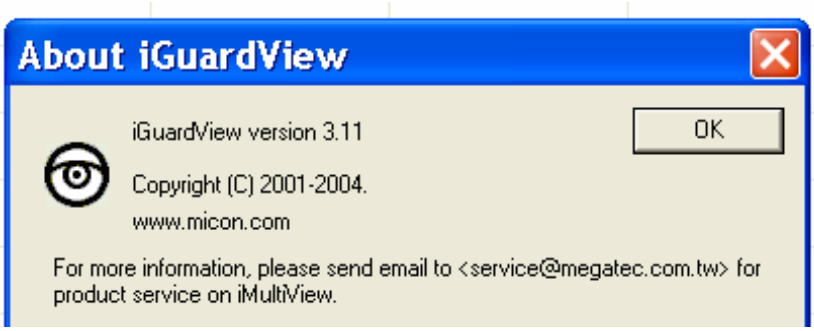


: Set the SNMP Parameter.



4.2.2.9 Help

Help : Display iGuardView version, Copyright information and product service contact.



Chapter 5: iGuard Web Manager

5.1 Introduction

If you have connected the iGuard to an internal network with a DHCP server, the IP property (IP address, Mask, and Gateway) will be automatically assigned.

1. Start the Web Brower (Netscape or Internet Explore)

2. Enter the iGuard IP Address(e.g. 192.168.0.30) and press ENTER as in Fig.6

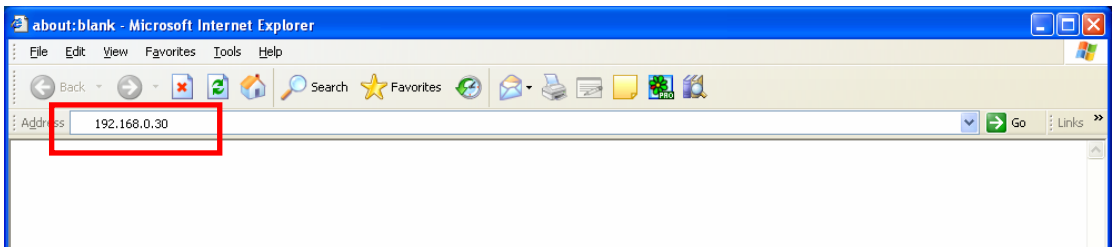


Fig.17 Enter iGuard IP address

3. A login screen will appear as in Fig.7. The default login is “admin” and the password is the CD Key that has been placed on the CD sleeve.

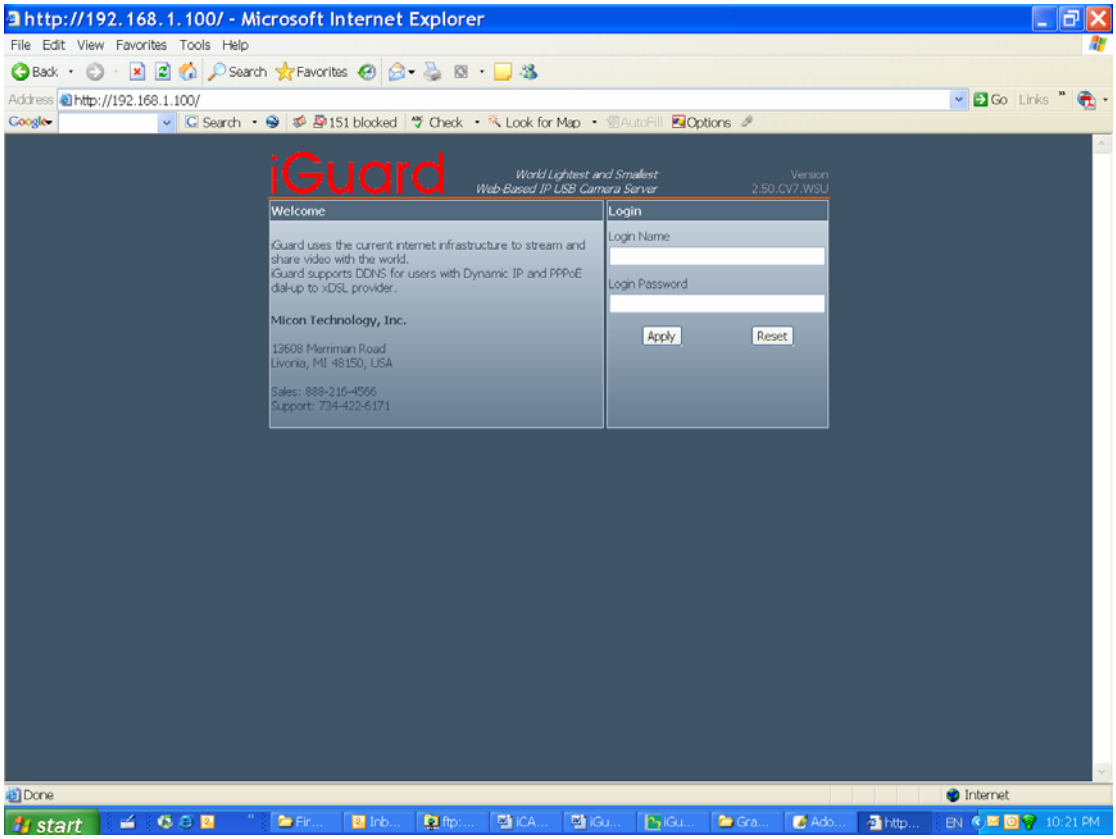


Fig.18 iGuard Login screen

5.2 iGuard Web Manager Interface

The iGuard webpage main menu is divided into two sections. The selection menu on the left and display menu on the right. The selection menu consists of the following options:

- **Web-Camera Selection**
- **Information**
- **Basic Settings**
- **Advanced Settings**

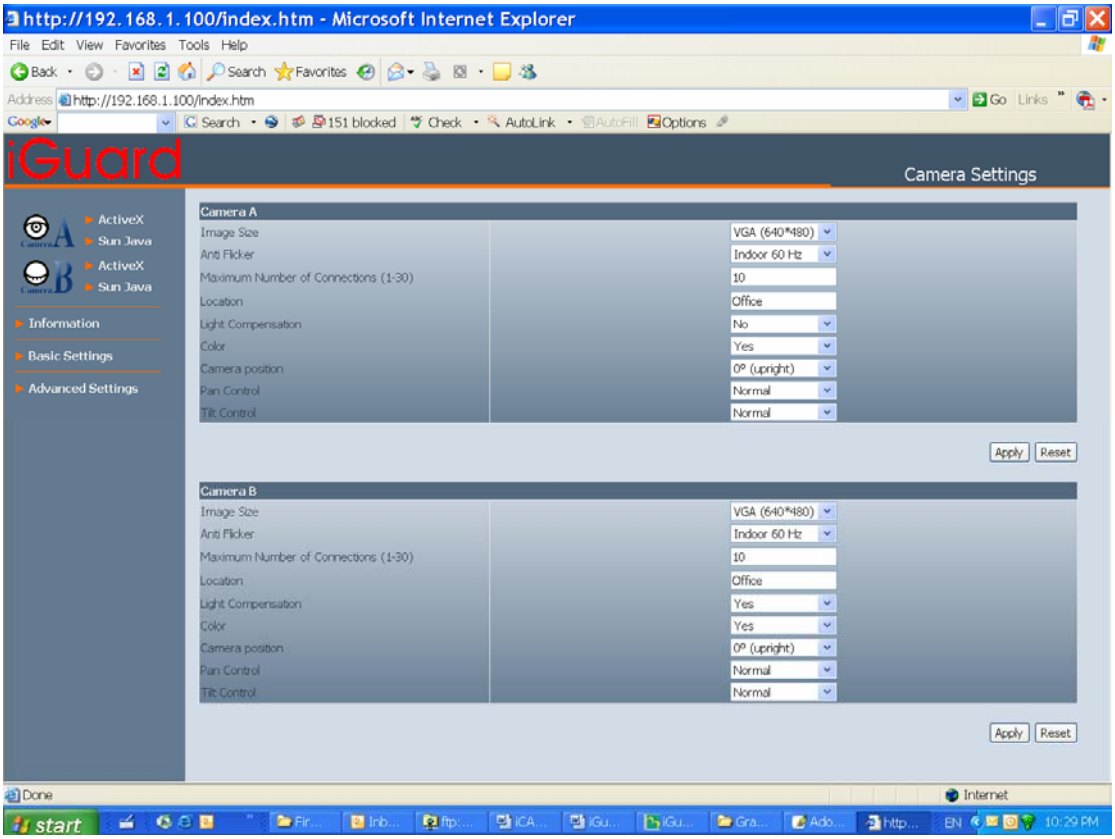


Fig.19 iGuard Web Manager Main Menu

When using iGuard for the first time, you must set the following to ensure that iGuard works properly;

a. Set the necessary parameters in the “Configuration” menu. In particular, the “Anti Flicker” under “Camera Settings” should be set to 50Hz or 60Hz (change this to 60Hz or 50Hz / Outdoor if video output continues to flicker).

b. That the USB PC camera lens is adjusted to the correct focal length for best results.

By default the above Camera Settings page is displayed when you login.

5.2.1 Web-Camera Selection

Click on either “ActiveX” or “Sun Java” from Camera A or B to view the camera images.

By default the first USB camera connected to iGuard will be denote as “Camera A”

Click “Camera B” to view camera B.

Note: ActiveX can only function on Windows platform and a plug-in has to be installed on the client's computer. If this is prohibited for safety reasons you will have to use Sun Java to view the video feed. Sun Java also allows users who are not using Windows based Operating System to view the video feed.

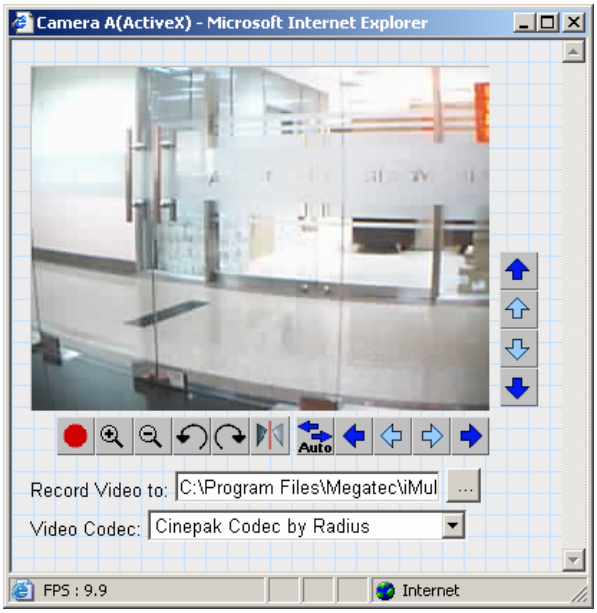
Once you click on “Camera A” the following image will appear.

Make sure to adjust the USB camera lens for best picture results.

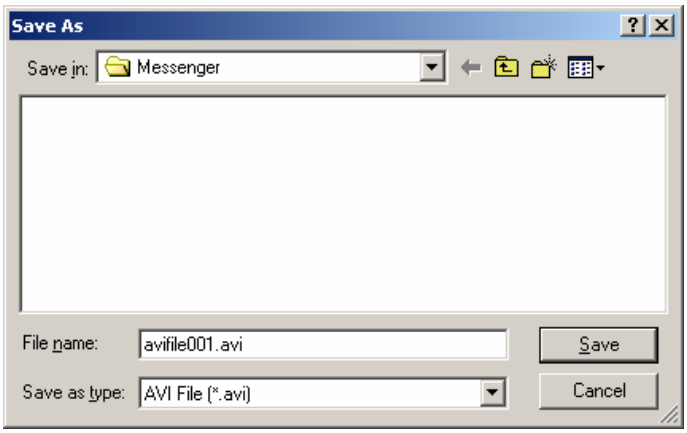
Click on the controls along the Window to control the camera.

Note:

The pan and tilt controls will only work with cameras which has this function built-in.



Click  to record the current image to the selected directory. To change the saved location and filename. Click  and the “Save As” window will pop up. Choose an alternate location and filename. Click the “Save” button to confirm changes.



To change Video Codec, click 

Note: The availability of Codec depends on weather the individual user has it installed on the PC or not. Download and install Windows Media Player 10 to enable MPEG4 codec.

 Digital Zoom In, Digital Zoom Out

 Rotate Left, Rotate Right

 Flip the image vertically.

Auto Pan the camera

 Pan Left by 5 deg / Pan Left by 1 deg.

 Pan Right by 1 deg / Pan Right by 5 deg.

 Tilt Up by 5 deg / Tilt Up by 1 deg.

 Tilt Down by 1 deg / Tilt Down by 5 deg.

Note: The above Pan/Tilt button will only work with cameras supporting the Pan/Tilt function

5.2.2 Information

5.2.2.1 System Status

This displays all the information relating to iGuard.

i. System Information

This shows iGuard System Information such as the Hardware and Firmware Version, the serial number, current / local System Time, the system name, contact, location and uptime. These values are either provided by iGuard or set by user.

ii. Network Status

This shows iGuard Network settings. The MAC Address is unique to every iGuard. All the other values are set by the user in Setup Wizard.

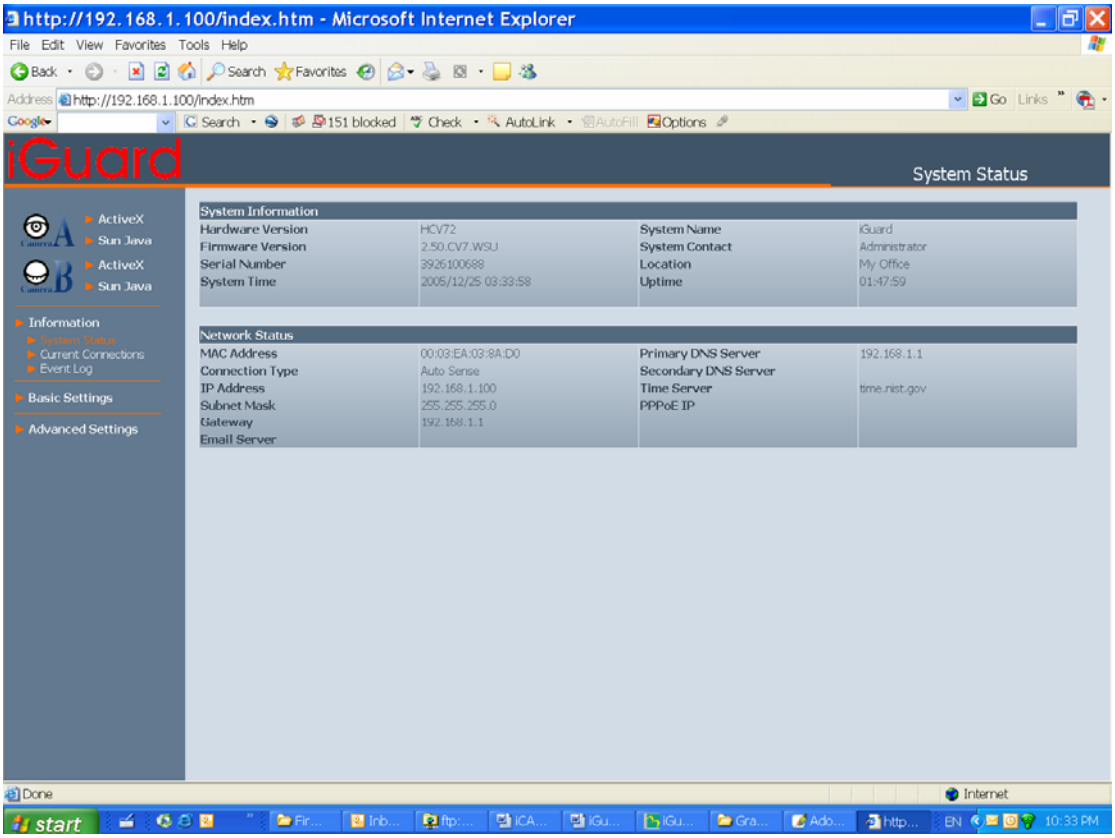


Fig.20 iGuard System Status

5.2.2.2 Current Connections

This will show all the users currently viewing either Camera A or Camera B. It also lists, the login time, and total bytes received. The user has an option to block the IP or even disable the account of any errant viewer. The administrator privilege will be required for this feature. A total of 10 connections can be displayed at the same time.

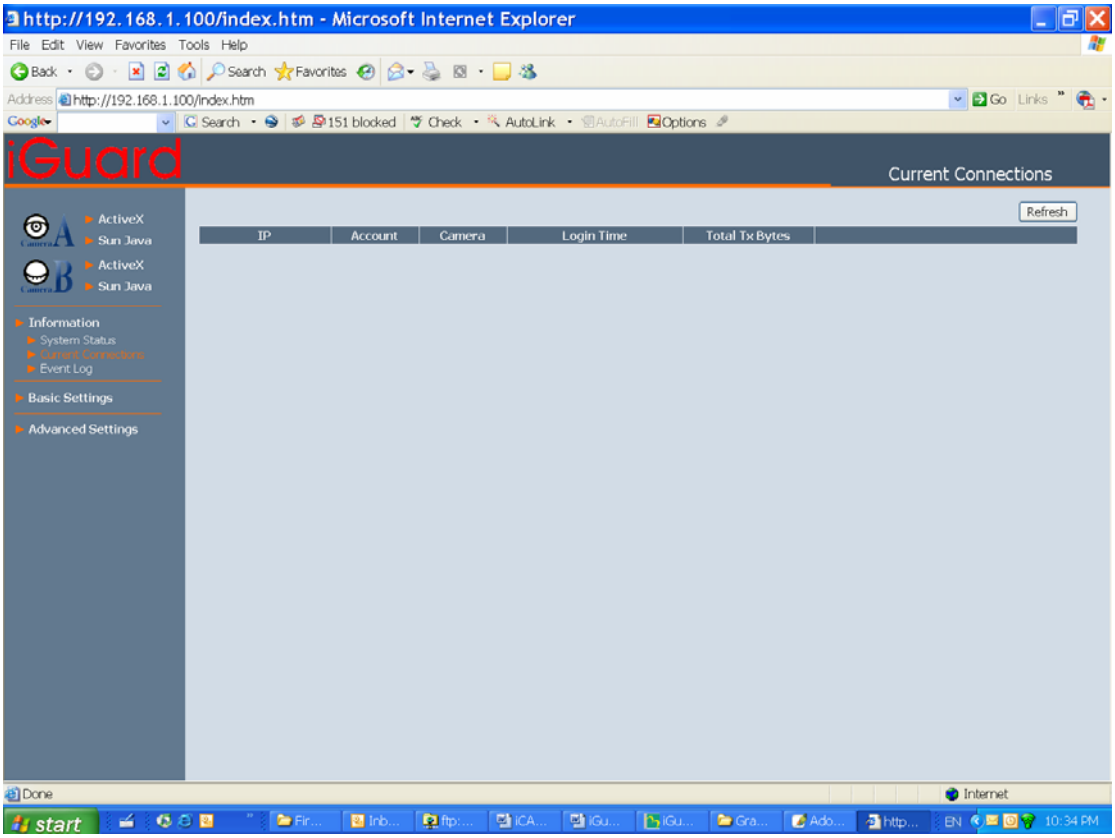


Fig.21 iGuard Current Connections

5.2.2.3 Event Log

This will keep a record of all events that occurred in iGuard. The user can Refresh, Clear or Save the log file. There is also an option to sort the logs according to "Level" or "Type"

iGuard can log up to 2,000 events

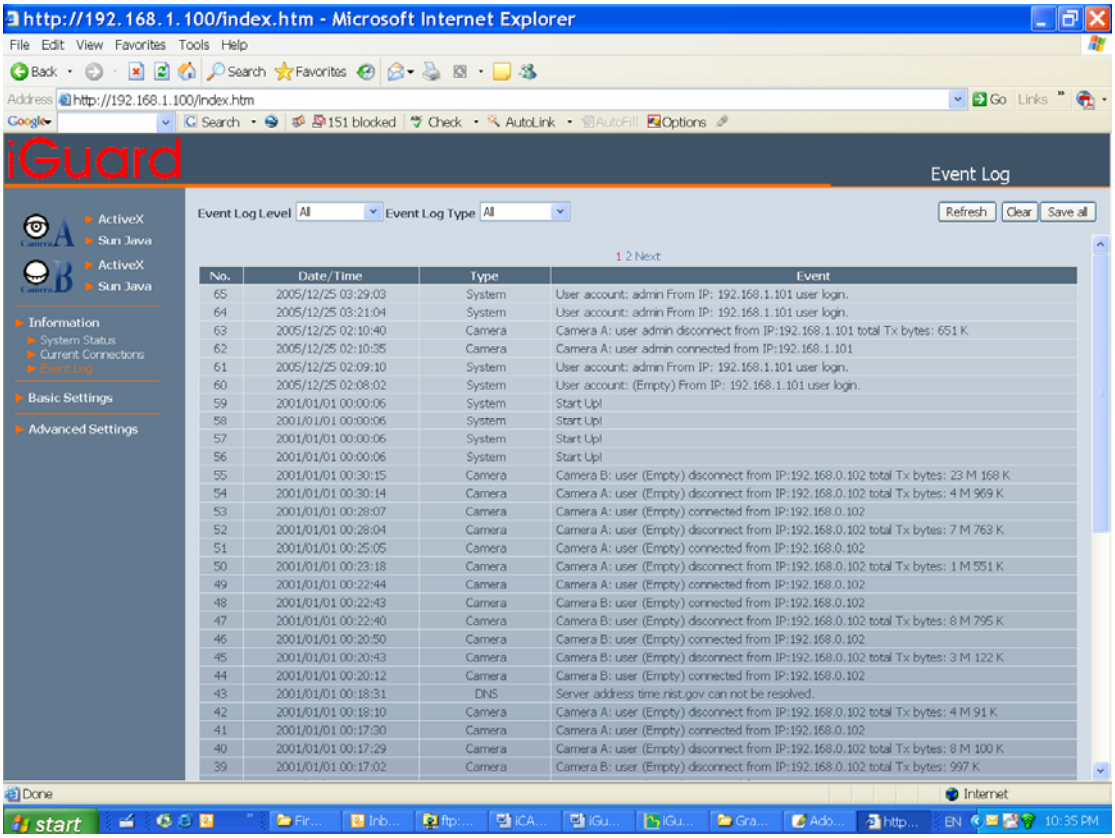


Fig.22 iGuard Event Log

5.2.3 Basic Settings

5.2.3.1 Camera Settings

Use this to set up the USB camera.

i. Setting up Camera A (Similar with Camera B)

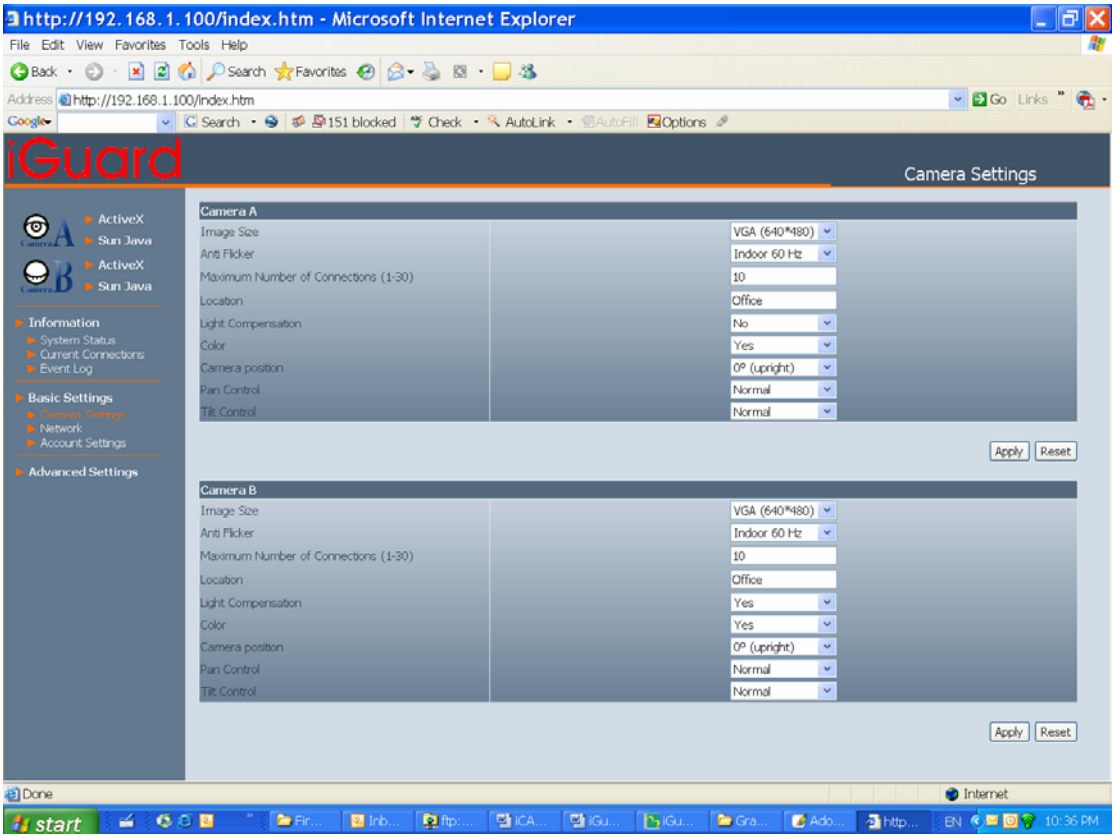


Fig.23 Individual Camera Configuration

"Image Size"

Choose between 640x480, 320x240,etc. The higher the image size, the better the image quality, the slower the frame rate for network transmission.

"Anti Flicker"

Choose between 50Hz, 60Hz or Outdoors. Note: If you do not choose the right frequency, the image will flicker or lines will appear on the images.

"Maximum Number of Connections (1-30)"

Use this to limit the number of users that can connect to this camera.

"Location"

Enter a suitable location / name for the camera.

"Light Compensation"

Choose "Yes" and iGuard will increase the lighting of the image. This is useful when monitoring indoors.

Choose "No" if you do not want iGuard to adjust the light and view the images as is.

"Colour"

Choose "Yes" for colour and "No" for black and white display.

"Camera Position"

Choose from the automatic “0 degree (upright)”, to 90, 180 (upside down), and 270 degree position of the camera. This is to facilitate the ability to reposition the camera in any way the user desires.

“Pan”

Choose between “Normal” for regular placement or “Reverse” when the camera is placed upside down.

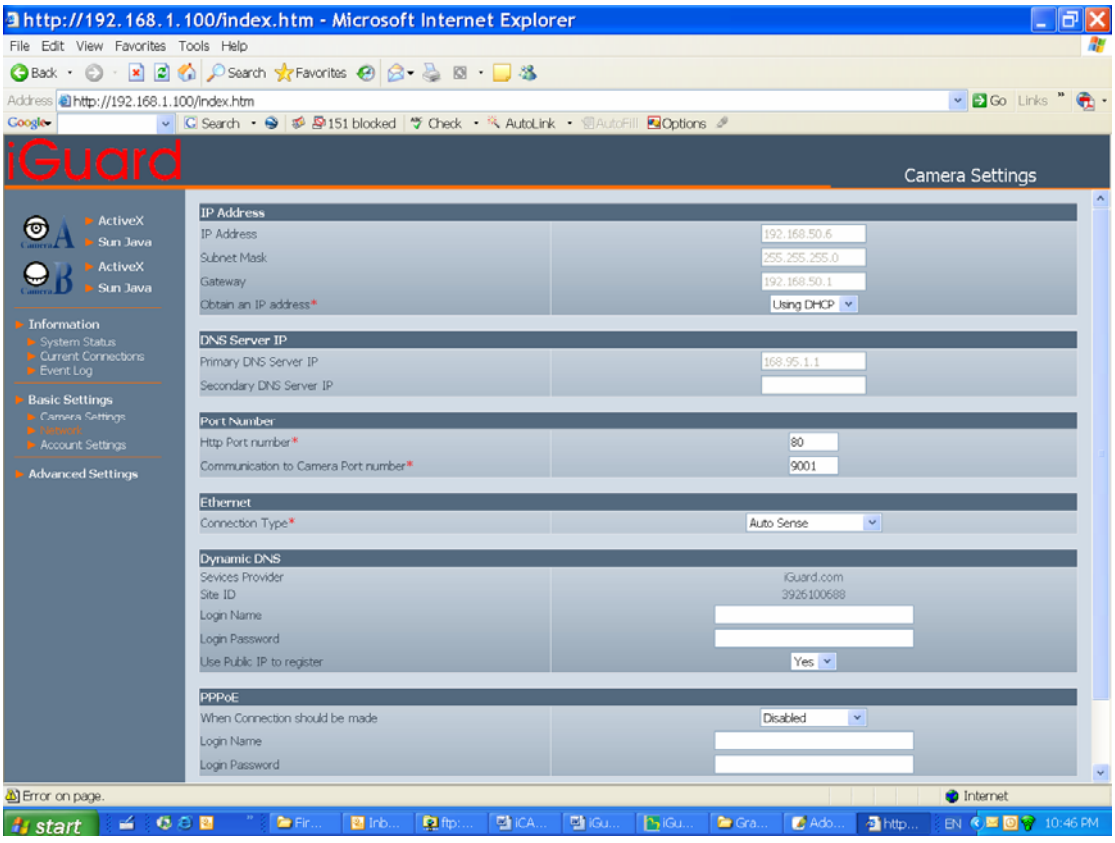
“Tilt”

Choose between “Normal” for regular placement or “Reverse” when the camera is placed upside down.

Click “Apply” to save changes. Otherwise, all changes will be lost.

5.2.3.2 Network

This option determines the iGuard Network settings.



i. IP Address

By default, the IP address is set to be automatically assigned by DHCP server. If you have a static IP, you can enter the new address here and click “Apply” to change **(Note: you will lose connection to the iGuard if the IP is changed)**.

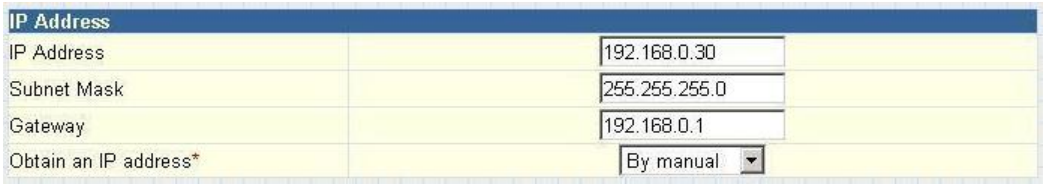


Fig.24 iGuard IP Address Settings

"IP Address"

This item determines iGuard IP Address.

"Subnet Mask"

This item sets iGuard Subnet Mask. The value is normally 255.255.255.0

"Gateway"

This item is to set iGuard Gateway.

"Obtain an IP address"

This allows the user to choose either to set iGuard IP Address manually or via DHCP. iGuard will reboot after the above settings have been changed.

ii. DNS Server IP

Fig.25 iGuard IP DNS Server IP

"Primary DNS Server IP"

This item sets iGuard primary DNS Server IP address.

"Secondary DNS Server IP"

This item sets iGuard secondary DNS Server IP address. iGuard will use the secondary DNS Server IP address if the Primary DNS Server IP address is not working.

iii. Port Number

Fig.26 iGuard Port Settings

"HTTP Port Number"

By default the port number is 80. You have to use a different port number here if you host a website on the same network, if your ISP blocks port 80 traffic, or if you have multiple iGuard on the network

"Communication to Camera Port Number"

By default the port number is 9001.

iv. Ethernet

Fig.27 iGuard Ethernet Settings

"Connection Type"

This item sets the communication speed between iGuard and the Network. iGuard will reboot after "Connection Type" is changed.

v. Dynamic DNS

If you use a consumer grade broadband service, the chances are you will have a dynamic IP address. You will need to subscribe to a DDNS service to keep track of this ever-changing IP address if you would like to use the remote monitoring function of iGuard.

Fig.28 iGuard Dynamic DNS Settings

"Service Provider"

As value added service, iGuad.com hosts a DDNS server that tracks iGuard's IP address if it was changed for any reason. Before you use this function, you will have to register on :www.iguard.com.

Your can also track your IP address by subscribe to other DDNS services via the DDNS client built-in your router..

"Login Name (site name)"

Enter the "login name" you used when you registered on www.iguard.com

"Login Password"

Enter the Password you selected when you registered on www.iguard.com

"Use Public IP to register"

Choose "Yes" or "No".

vi. PPPoE

If you use a dedicated DSL internet service, use this option to directly dial-up your DSL modem and connect to the Internet.

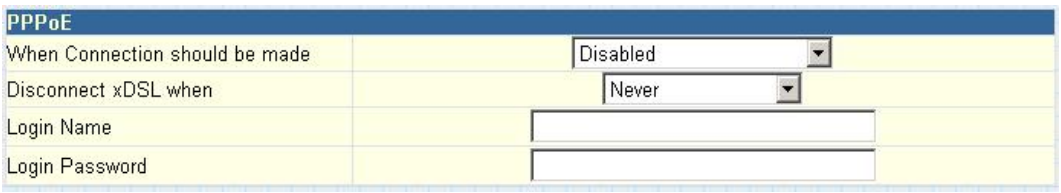


Fig.29 iGuard PPPoE setting

"When Connection should be made"

The user has a choice of;

Disabled	:	Default setting. iGuard does not dial in
Connect always	:	iGuard will automatically dial in.

"Login Name"

Enter the login name assigned by your ISP.

"Login Password"

Enter the password assigned by your ISP.

5.2.3.3 Account Settings

This allows you to set up to Eight (8) user account with different permissions for iGuard.

WARNING: You **MUST** set an Administrator account **BEFORE** setting either "Operator", "Viewer" or "No Access". Failure to do so will result in you being locked out of iGuard Web Manager! You will have to refresh your firmware to be able to use the iGuard again

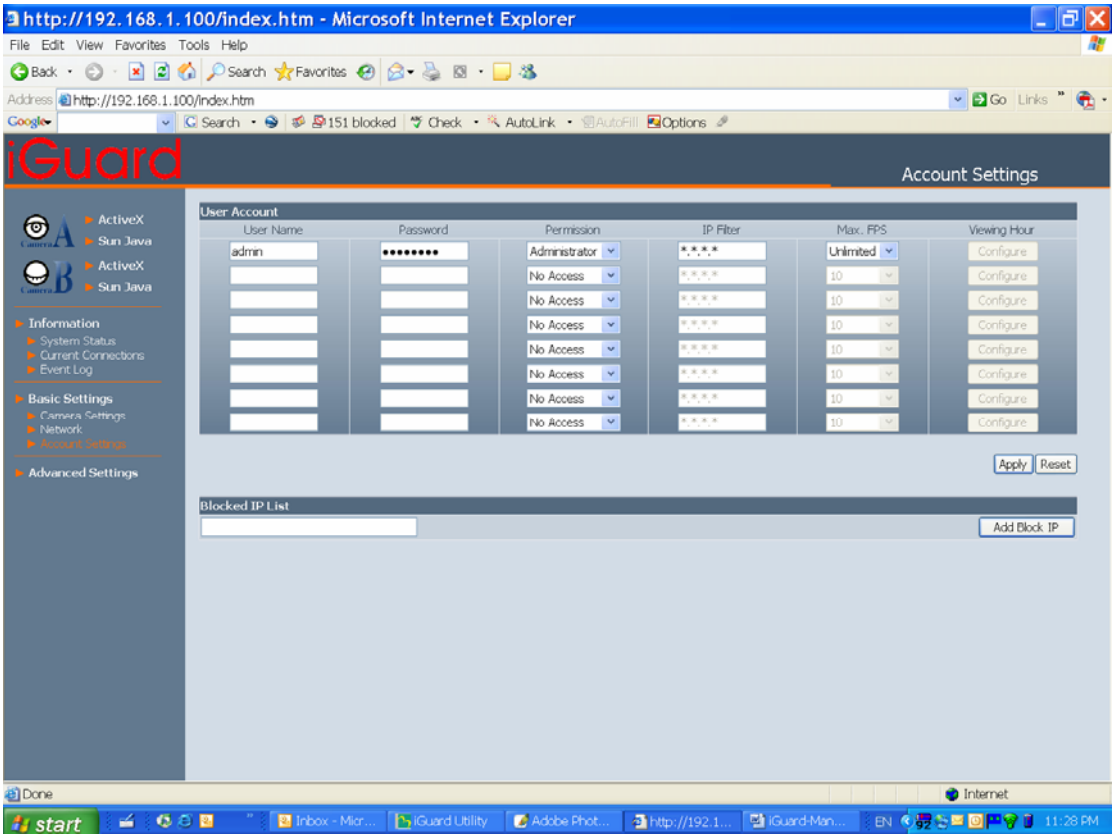


Fig.30 iGuard User Account Setting

i. User Account

"User Name"

Determine the username of visitors who can log in. The administrator can set up to 32 case sensitive character names.

"Password"

Set a password for the visitor's account. The administrator can set up to 32 case sensitive passwords.

"Permission"

Determine the permission level to one of "Administrator", "Operator", "Viewer" or "No Access"

Administrator:	This permission allows the user full access including write permission to all the sections.
Operator:	This permission level allows the user access to iGuard menus, but without the permission to amend them. The administrator can also set "Permit Hours" here for seeing camera.
Viewer:	This permission level allows the user to access iGuard at specific time as set in "Permit Hours" for seeing camera. The user does not have write permission and only access the "Web Cam" and "Information" section.
No Access:	This is to revoke either of the above two permission levels given to a user. And make the user account disable.

"IP Filter"

Visitor can only login from the IP address specified here for security consideration. You can restrict a user access only from 192.168.1.0/24 by setting up "192.168.1.*". Otherwise, leave it as "*.*.*.*" to allow the user to login from any place.

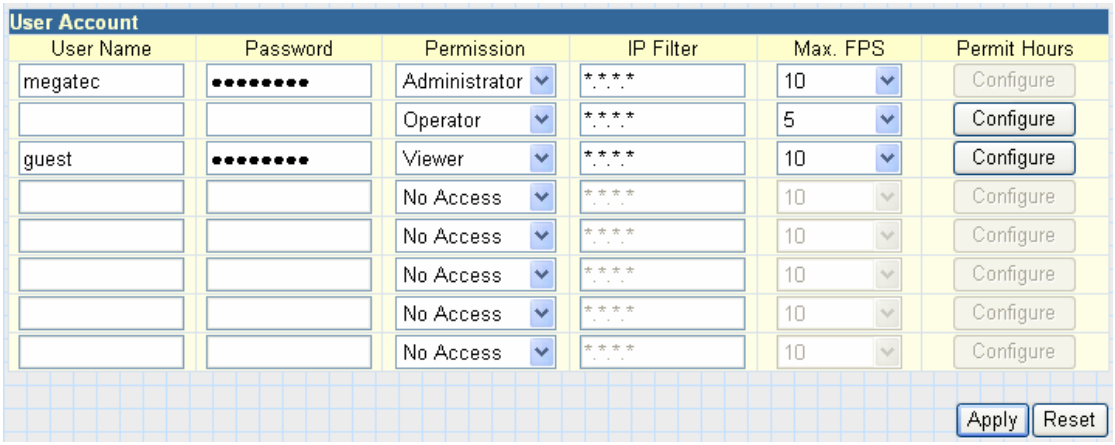


Fig.31 iGuard User Account Settings

"Max FPS"

This allows the administrator to determine the frames per second ("FPS") allocated to each type of account. By limiting the FPS, the administrator can manage the limited bandwidth available. The administrator can set a figure between 1 to 20 and unlimited FPS.

"Permit Hours"

When the Permission level is set to either "Operator" or "Viewer", the Administrator can configure and determine the time to which either permission level can access the camera.

Click "Configure" to bring up the following window. You can set up to 4 different Permit Hours (in 24hr format). Click "Apply" to save and "Close" to exit.

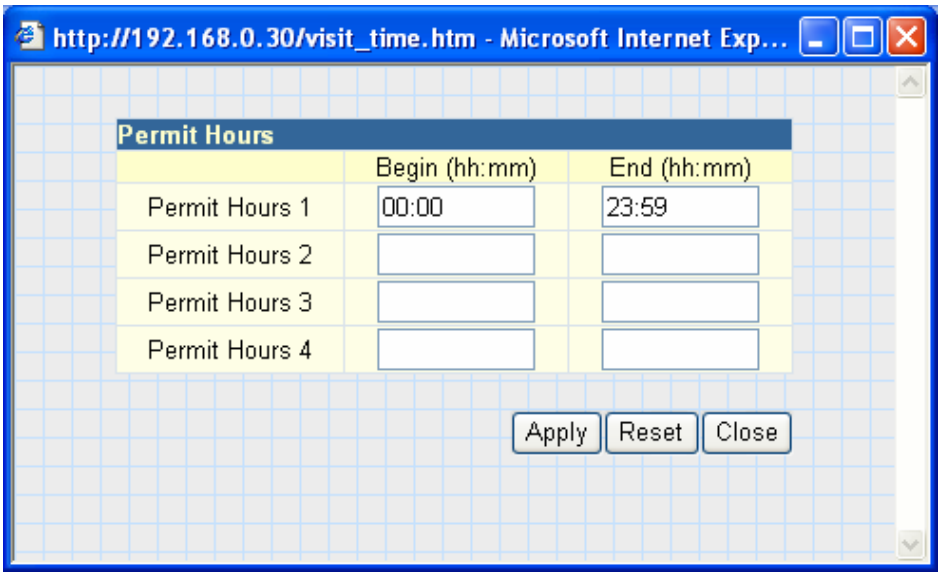


Fig.32 iGuard Permit Hours Configuration

5.2.4 Advanced Settings

5.2.4.1 Event Notification

This determines the type of event an email is sent by iGuard. iGuard can send notifications to up to 8 email recipients. Note: You must have Administrator privilege to edit this section.

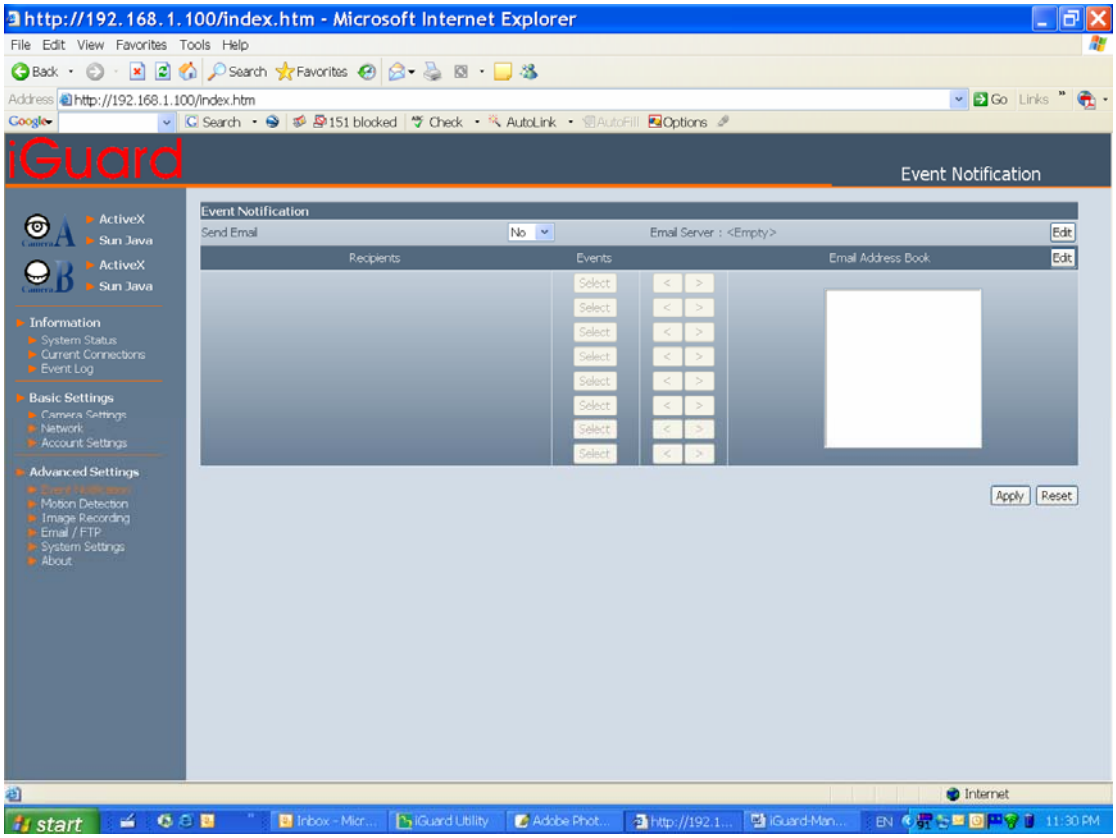


Fig.33 iGuard Event Notification Page

i. Event Notification

"Send Email"

To activate Event Notification, you will need to set "Send Email" to "Yes". Select "No" if you do not wish to send out any notification.

"Email Server"

A valid "Email Server" with username and password (if authentication is required) must be made available for this feature to work. If you do not have this setup, or wish to change the settings, click on "Edit".

"Email Address Book"

There must be at least one valid email address in the address book. The default email is just a sample. If you wish to add or delete entries in your address book, click "Edit".

"Recipients"

iGuard can send email notification to up to 8 valid email accounts. To add an email to the recipient list, click < . To remove, click > .

"Events"

This determines the events that the selected recipients will be notified of by email. There are three types of events, Information, Warning and Error. Click

Select to select from the list of events you wish these recipients to be notified of.

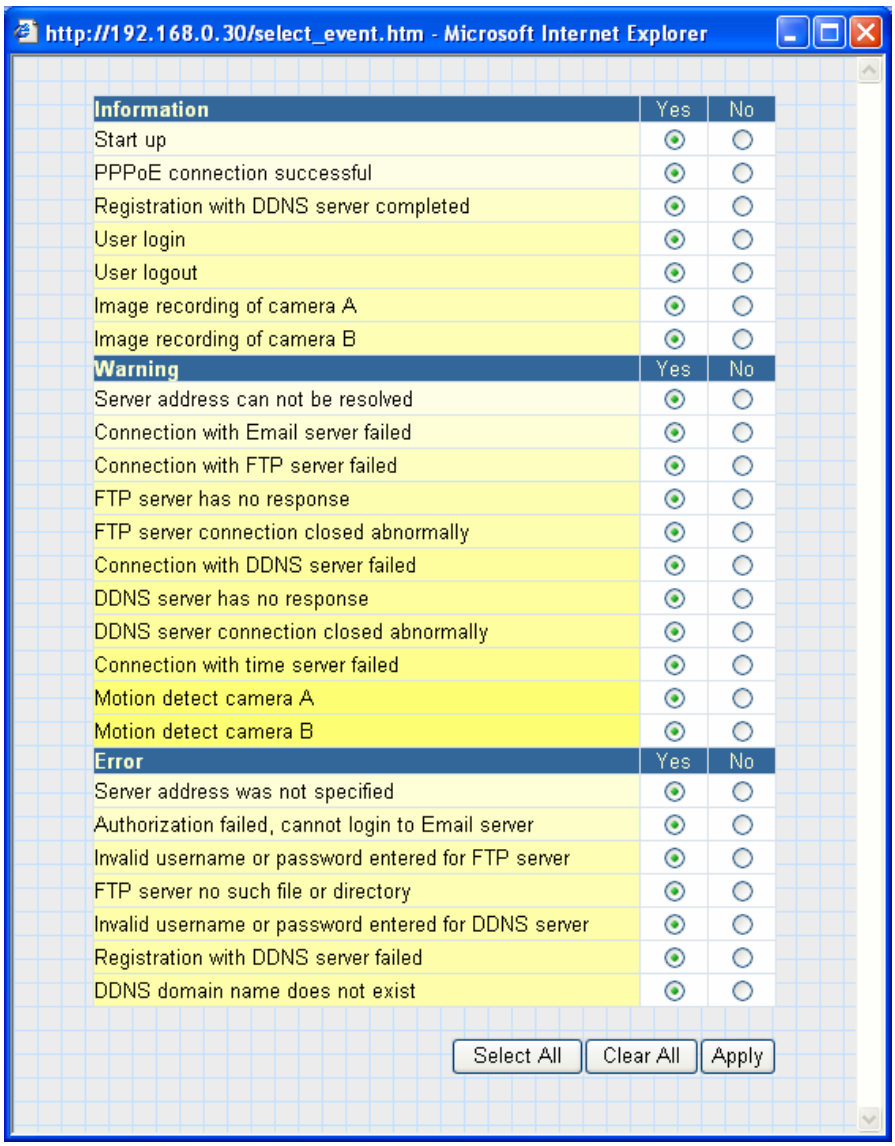


Fig.34 iGuard Event Selection List

By default, all the events are selected; you must click “Apply” to activate them. Close the window to return to the Event Notification Page. Click “Apply” to save your settings.

iGuard will send you the following email notification depending on which event you have selected.

Note: The image recording and motion detection notification function here will send an email notification WITHOUT any pictures attached. For email notification with images, the administrator has to setup the Image Recording Page and Motion Detection Page under Advanced Settings.

Samples;

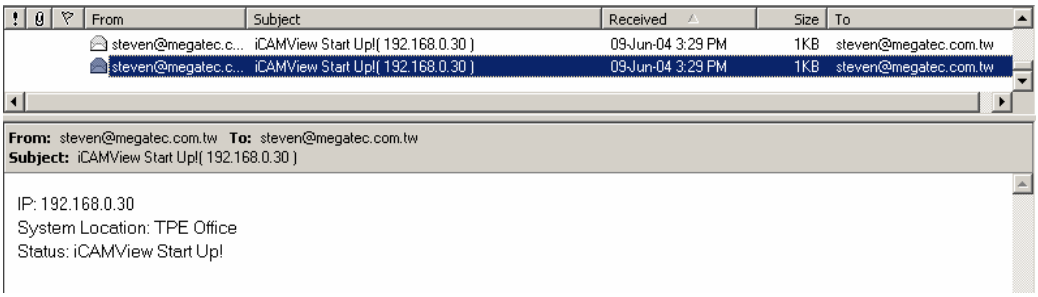


Fig.35 iGuard Event : Start Up

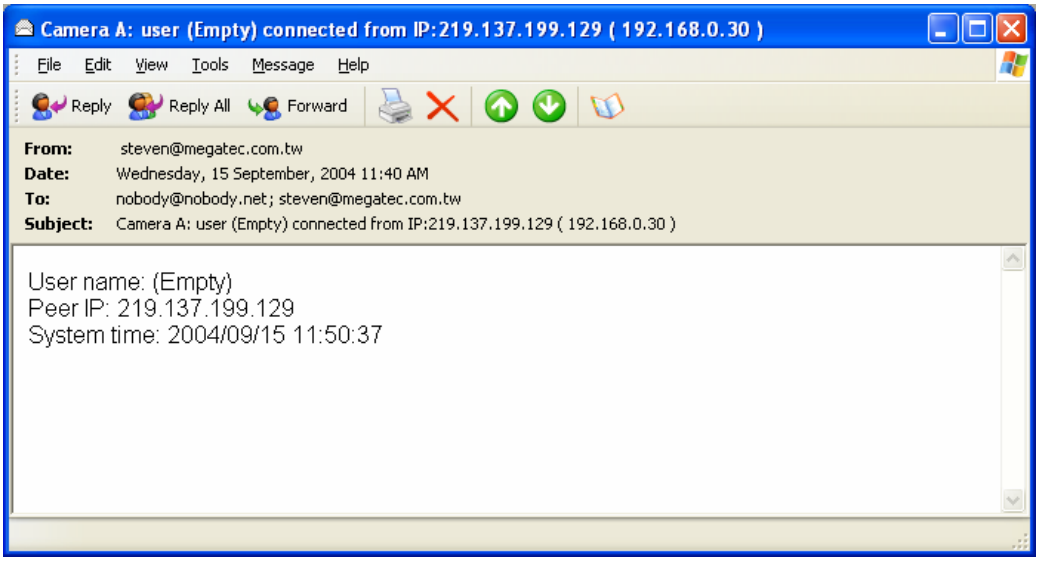


Fig.36 iGuard Event : User Login Details (Date, Time, Camera & IP)

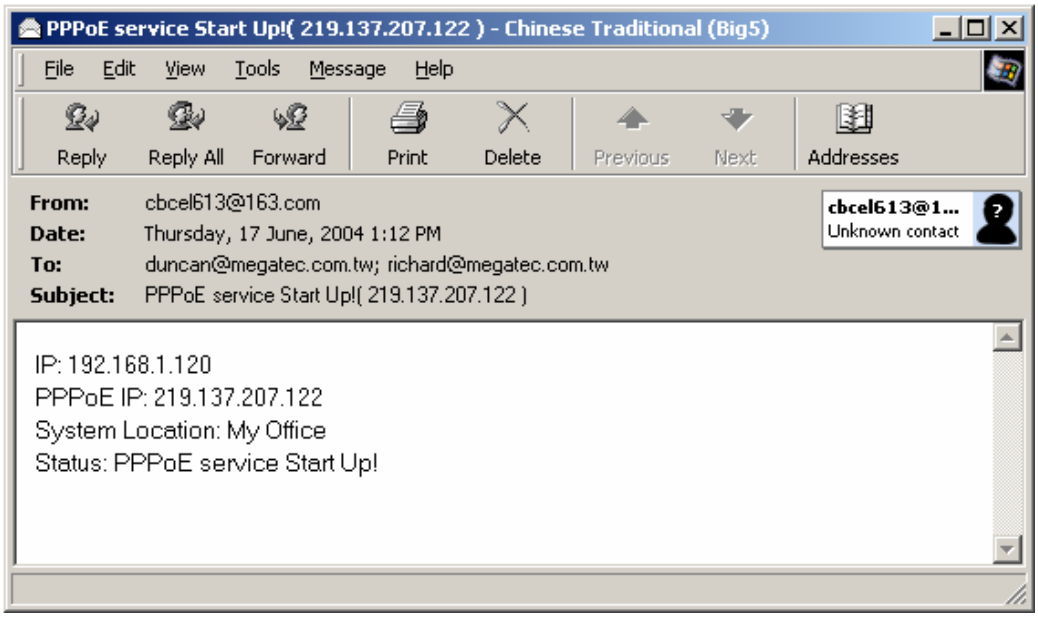


Fig.37 iGuard Event : PPPoE Connect Successful

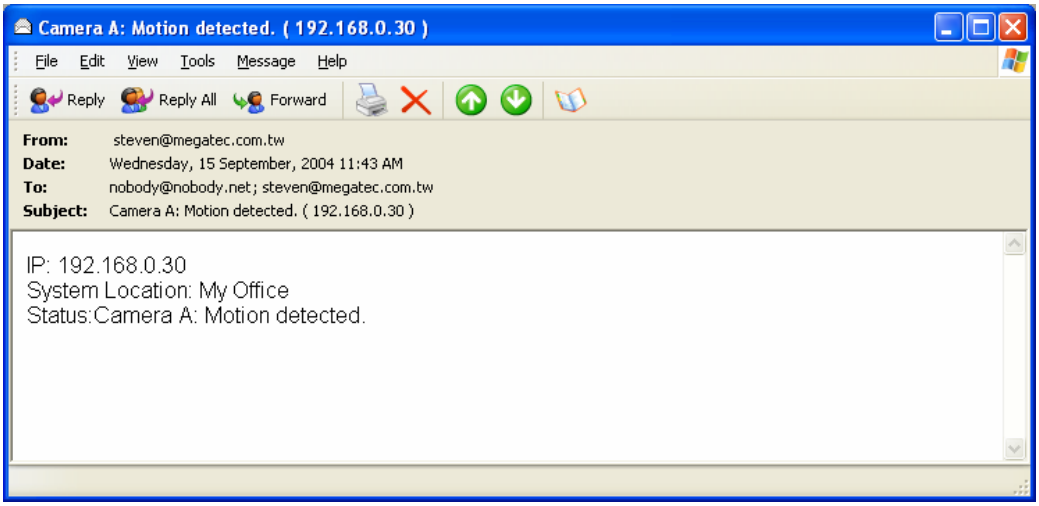


Fig.38 iGuard Event : Camera A or B Motion Detected

5.2.4.2 Motion Detection

This page allows the administrator to set motion detection functions for the cameras.

i. Camera A (or Camera B)

"Enable"

To activate motion detect, the administrator has two options;

a. "Always On" or

b. "On Schedule", the administrator can set up to 4 different time slots for motion detection.

"Detection Sensitivity"

This will determines level of change before motion capture is triggered.

"Send image every"

Select a value between 1 to 5 seconds.

"Stop sending emails after ## email(s) or image idle for ## second(s)"

iGuard will stop sending on the lower of the two conditions. You can set between 1, 3, 5, 7 and 10 seconds. Emails can be set from 1 to 99999 pieces, or 0 for stop sending email only when image idle occurred.

"Schedule"

If set to "On Schedule" in the above section, the administrator can then input the four preferred schedule time slots for motion detection. Time must be entered in 24hr format.

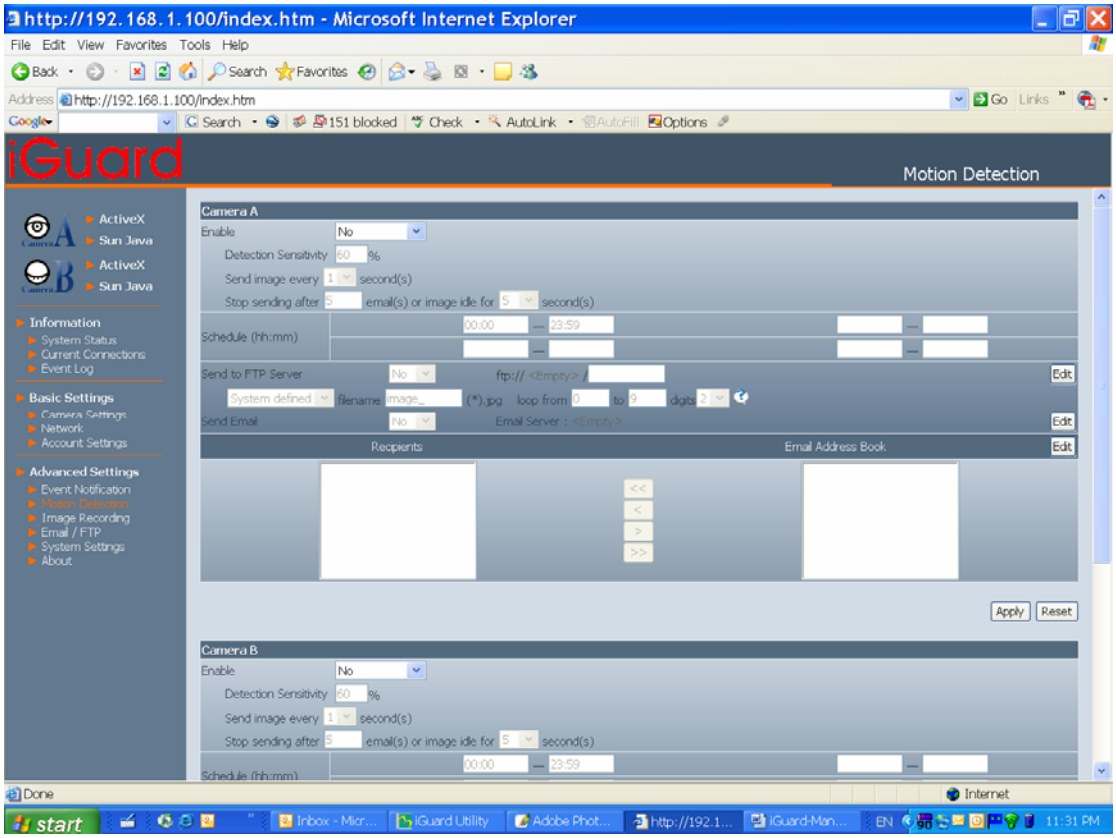


Fig.39 iGuard Motion Detection Page

“Send to FTP Server”

This option allows the administrator to send and store the motion detected images on a FTP site. This is useful for future reference and recording purpose. Click “Yes” to activate.

“ftp://<empty>/<folder>”

This box allows the administrator to determine the file location within the FTP site. If you have not entered a FTP server, the above will be left <empty>.

To setup the FTP server, click “Edit” to go to the Email / FTP Page. Once you have entered the FTP server, login name and password, click “Apply” and then Click on “Motion Detect” to return here.

Enter a directory or folder name in <folder>. Click “Apply” when done.

“System Defined / User Defined”

The administrator can also determine to either have the system automatically assign the filenames for the pictures saved. Or assign these filenames.

“Filename”

Give the motion detected JPG images a standard filename prefix, to be followed by looping number suffix.

"Loop from ## to ##"

This will determine the number of suffixes preceding the above filename. Once the last number is reached, the first file will be replaced by the most current image.

"Digits"

This will determine the number of digits assignable for the above number suffix. The administrator can choose to assign between 1 to 6 digits.

Click  for an example.

"Send Email"

To send an email notification of Motion Detection with image, choose "Yes", otherwise choose "No"

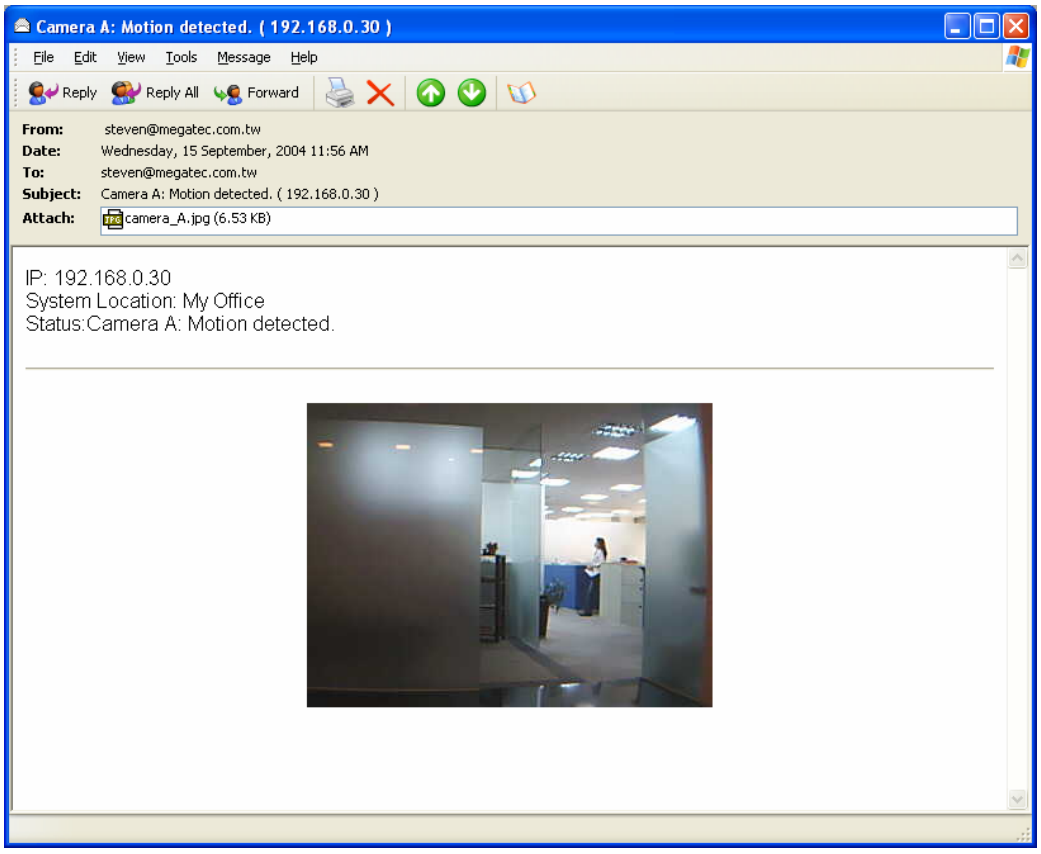


Fig.40 iGuard Motion Detect Email Notification

"Email Server"

The administrator will have to set this up. Otherwise, click "Edit" to go to the Email / FTP Page to make the necessary configuration. Click on Motion Detection to return here.

"Recipient" & "Email Address Book"

The administrator can determine who shall receive email notification. To add to the recipient list, either double click on the email in the address book or click

< . To add all the email address at once, click << . To remove an entry click >, or >> to remove all entries from the recipient list.

Click Apply to confirm and save the above settings.

5.2.4.3 Image Recording

Image recording allows the user to receive an image to either their email account or to a FTP server. The images will be sent over a predetermined interval and a certain period.

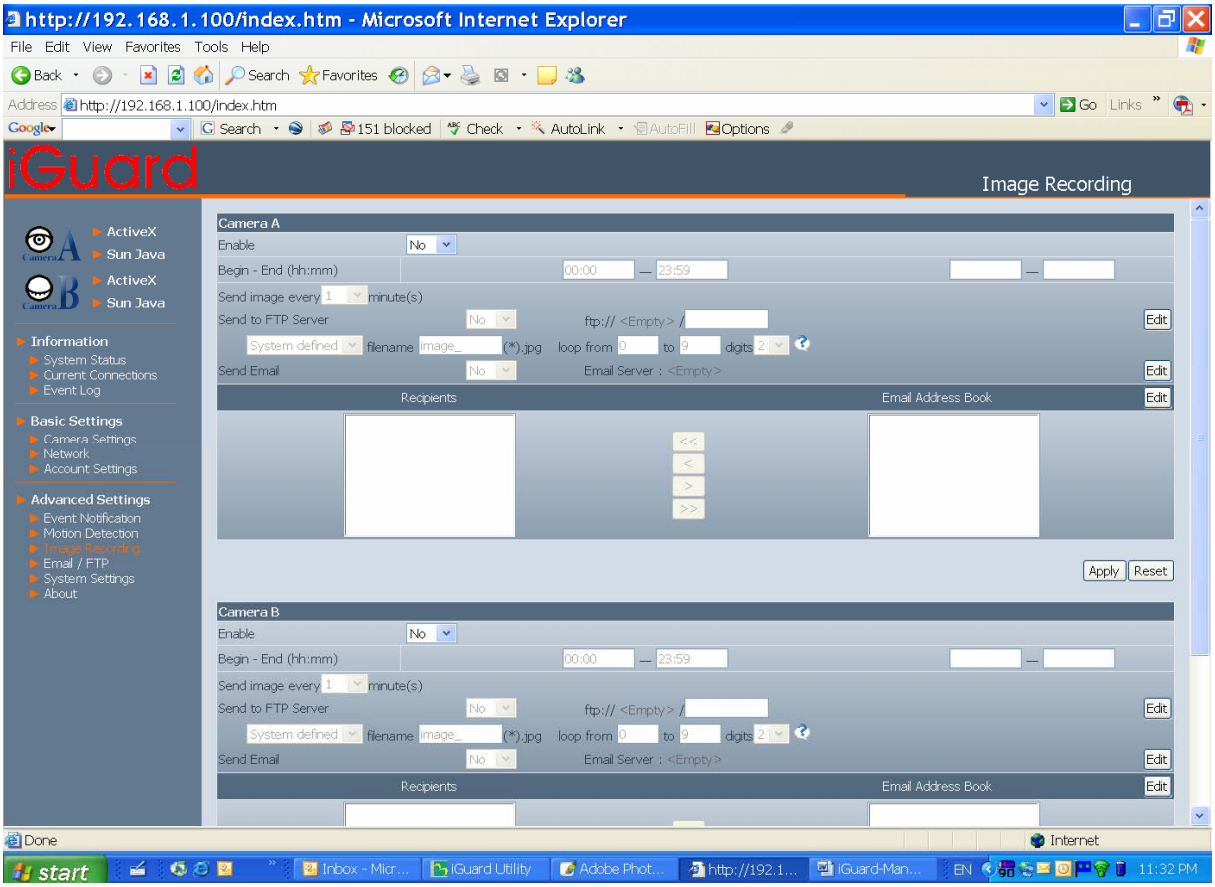


Fig.41 iGuard Image Recording Page

i. Camera A (or Camera B)

"Begin – End (hh:mm)"

The administrator can determine up to 2 time slots when Image Recording is active. The time is in 24hrs format.

"Send image every ## minute(s)"

The administrator can determine the exact interval at which iGuard capture and send an image. Choose among 1, 3, 5, 7 and 10 minutes.

"Send to FTP Server" & "Send Email"

This is similar to the function available in Motion Detection Page. Please refer to 4.2.4.2 for details.

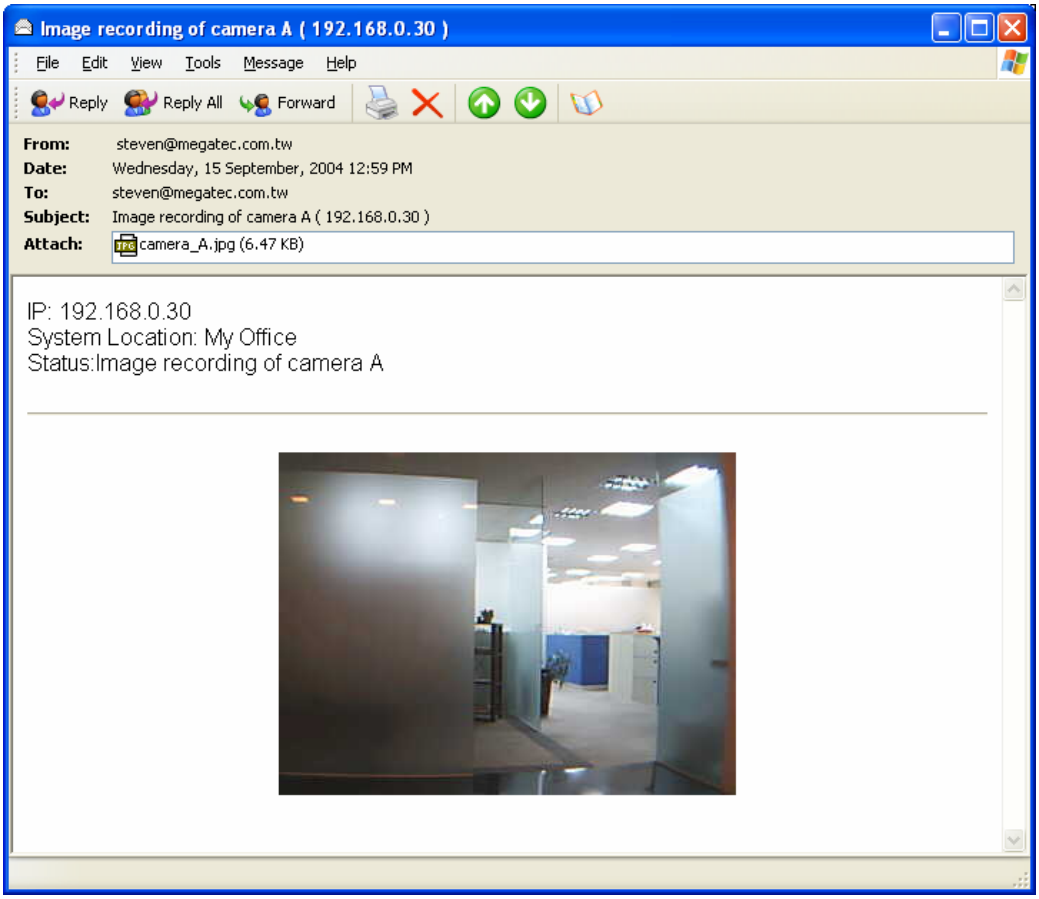


Fig.42 iGuard Email of Image Recorded

5.2.4.4 E-mail / FTP

This sets up the necessary Email and FTP server information. The administrator will have to enter a valid Account Name and Password to the Email server and/or FTP server. This information is necessary to allow email notification and ftp file sending features in Advanced Settings.

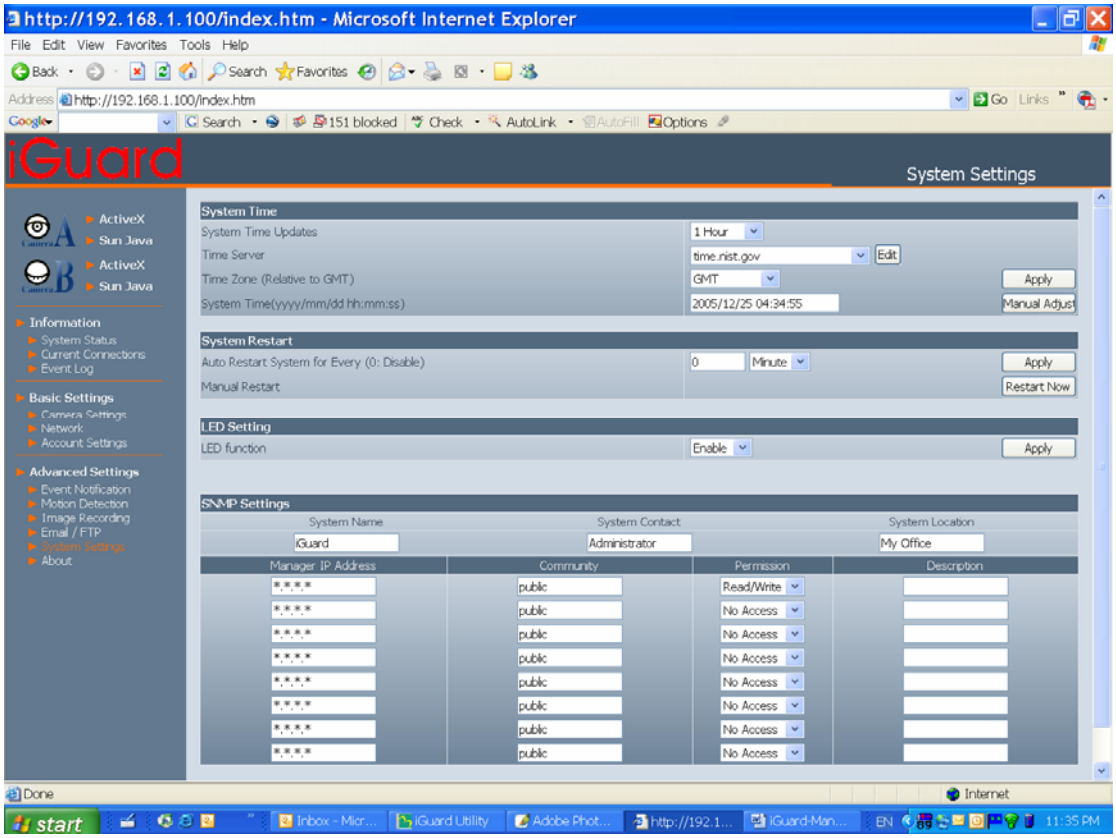


Fig.43 iGuard Email / FTP Page

i. FTP Settings

"FTP Server"

The administrator will have to enter the FTP server address here.

"Account Name"

Enter the FTP account name here.

"Password"

Enter the corresponding password.

Click "Apply" to save the above settings.

ii. Email Settings

"E-mail Server"

The administrator will have to enter the Email server address here.

"Sender's Email Address"

This will determines iGuard's Email address.

"Email Server Requires Authentication"

If set to “YES”, the administrator will have to provide the account name and password in order to access the Email server. Otherwise, enter “NO”.

“Account Name”

Enter the account name or login name to the Email server.

“Password”

Enter the password for the above account name.

Click “Apply” to save the above changes.

iii. Sending Test Mail

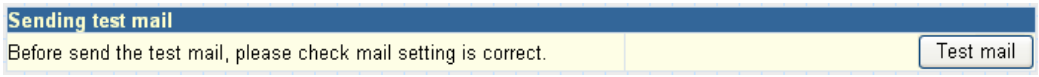
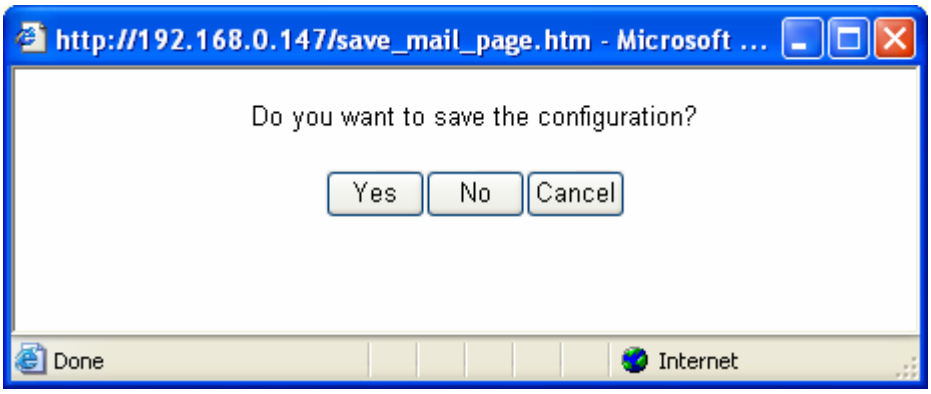
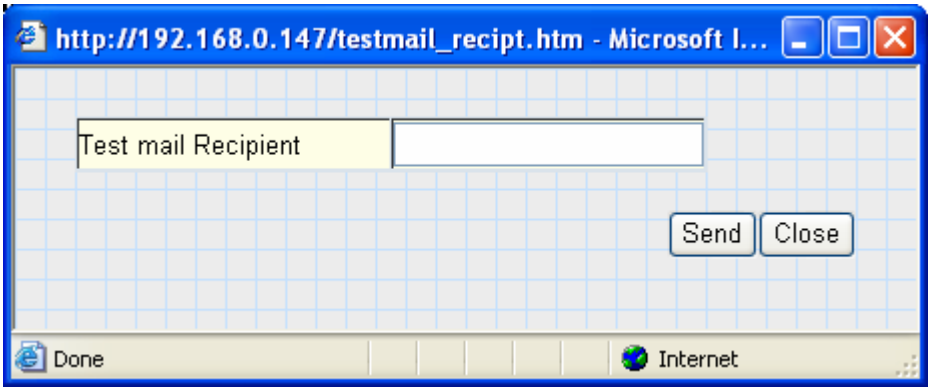


Fig.44 iGuard test mail function

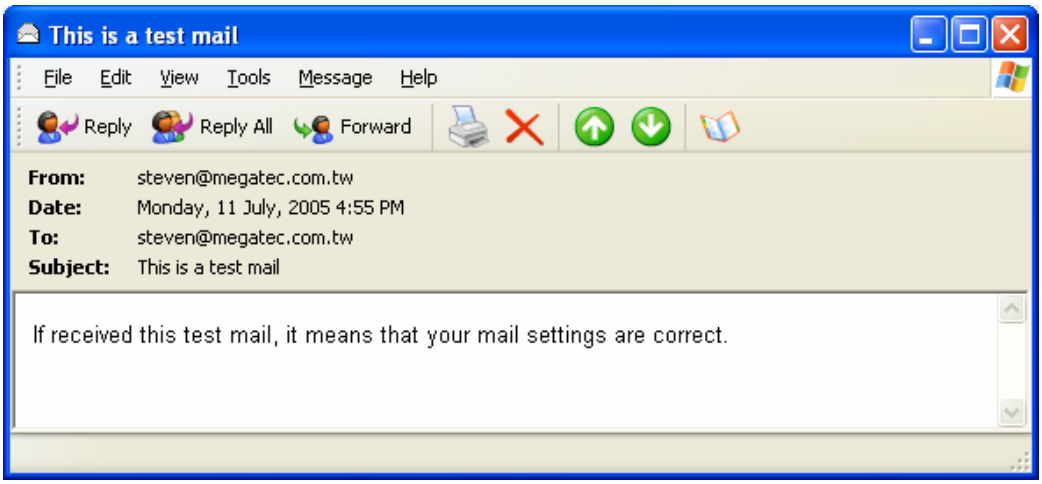
You must have the “Email Setting” configured to proceed with “Test Mail”. Once that is done click “Test Mail” and the following will appear.



Click “Yes” to confirm sending and the following window will appear.



Enter the “Test mail Recipient” email address and click ”Send”. If the Test Mail is successful, you’ll receive the following email message;



iv. Email Address Book

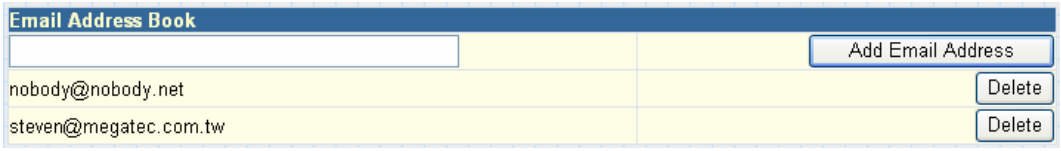


Fig.45 iGuard E-mail Address Book Entry

Enter an Email address in the box provided and click “Add Email Address”. The new email address will be added to the list. The administrator can store up to 20 email addresses here.

To delete an Email address, just press “Delete”.

5.2.4.5 System Settings

This page allows the administrator to set iGuard SNMP settings so it can be used by a NMS (Network Management System) like iGuardView.

i. System Time

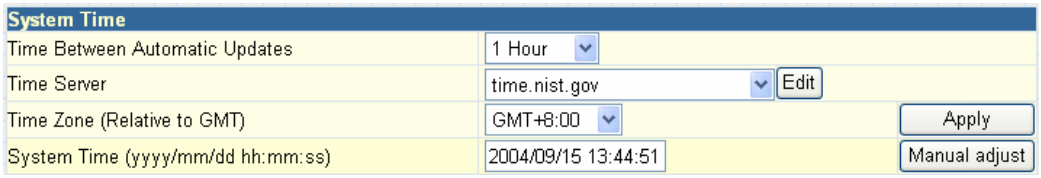


Fig.46 System Time

“Time Between Automatic Updates”

The administrator can set an interval for time synchronization. Select either 1, 3, 12 hours or 1, 10 & 30 days.

“Time Server”

Choose the nearest Time Server to your iGuard location. The administrator can choose from the list of a maximum of 30 Time Servers.

To add a new Timer Server the administrator must first make space by deleting some Time Servers. Once this is done, the add dialog box will appear as below. Click “Back” to return to the System Settings Page.

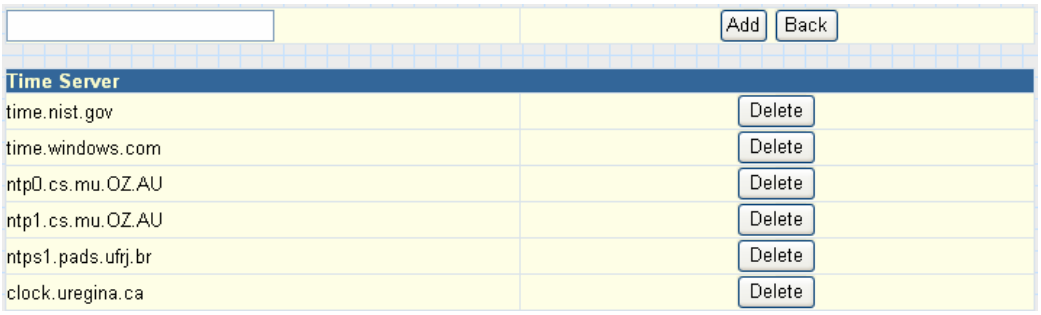


Fig.47 List of Time Server

“Time Zone (Relative to GMT)”

Select the appropriate time zone for your area. Click “Apply” to save.

“System Time (yyyy/mm/dd hh:mm:ss)”

This is to manually set iGuard System Time. The format is pre-determined to: yyyy/mm/dd hh:mm:ss. Click “Manual Adjust” to save any manual changes.

ii. System Restart

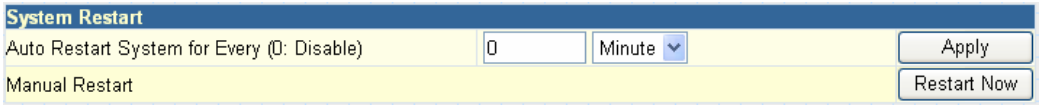


Fig.48 Auto Restart setting

“Auto Restart System Every”

The administrator can choose to restart iGuard at certain intervals (choose between minutes and hours only). This will ensure that iGuard will work smoothly. Click “Apply” to save changes.

“Manual Restart”

Click “Restart Now” to restart the system immediately.

iii. LED Settings

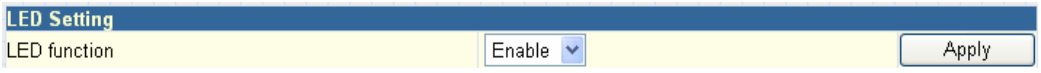


Fig.49 LED setting

“LED function”

The administrator can enable or disable the LED (except the Power LED) on iGuard here. Click “Apply” to save settings.

iv. SNMP Settings

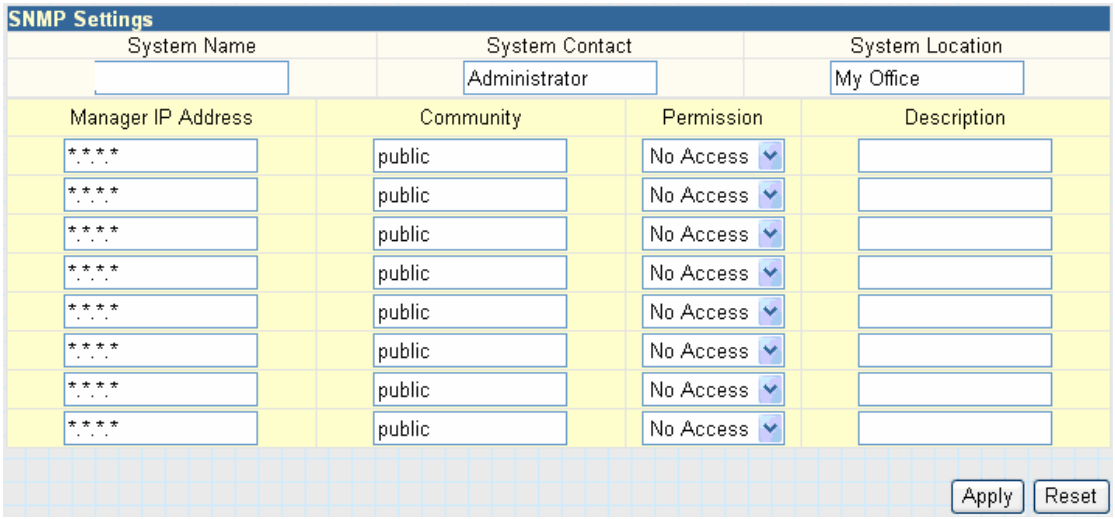


Fig.50 SNMP setting

”System Name”

This is to give iGuard a name identifiable in a SNMP network.

“System Contact”

This is to give the administrator a name.

“System Location”

This is to set iGuard location.

“Manager IP Address”

This set the IP address where the administrator can manage iGuard from. It is valid for up to 8 IP addresses. To manage iGuard from any IP addresses leave it as *.*.*.*.

“Community”

This is to set a Community name for NMS. The community name has to be the same as that set in NMS.

“Permission”

This is to set the administrator’s authority. Options are Read, Read/Write, and No Access.

“Description”

This is for an administrator to make notes.

“Enable”

Choose “Yes” to enable this feature or “No” to disable.

5. 2.4.7 About

The administrator can use this to check firmware information, save/restore settings, upgrade firmware and see manufacturer’s details.

i. About

This gives crucial information about iGuard's Firmware Version, Hardware Version and Serial Number. These are required information for service calls.

ii. Save / Restore Settings

"Save current Configuration"

Click "Save" to save the current settings and configuration to your PC. The text file will have a default format of YYYY_MMDD_####.cfg. The administrator can change this, if necessary.

"Restore previous configuration"

This function is only available if a setting has been saved initially. Browse to the location where the file is saved and click "Restore"

"Reset to factory default"

This function will reset all settings to its default value.

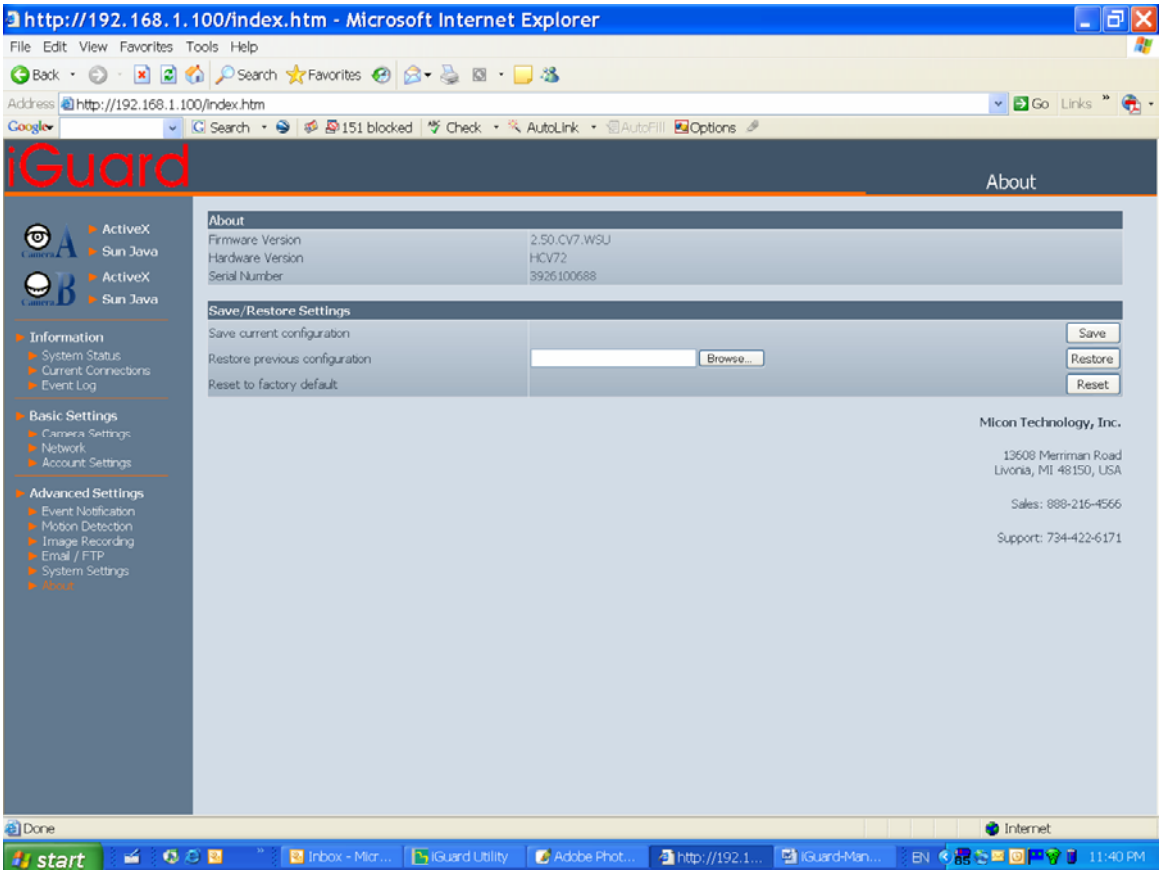


Fig.51 iGuard About Page

Appendix A: Router Configuration

If you have signed up a consumer grade broadband service, and you use a router to share your internet access, you will need to address following three major issues:

a. DDNS service
b. Port forwarding
c. Demilitarized Zone

If you are not familiar with those network terms, then you will probably need a network technician to help to setup the iGuard.

The following information assumes you have basic knowledge about networking and is for your reference only. Technical support for remote monitoring is only available to those who subscribe to the DDNS service provided by Web Surveillance, LLC

a. DDNS:

In order to access the iGuard from internet, you will have to know the external IP address of your iGuard. If you have a consumer grade broadband service, this IP address may change over time, making it impossible for the remote PC to communicate with your iGuard, just like you ask people to call you but you change your phone number without notified the other party. The solution is to subscribe to a DDNS service which keeps track of your IP address. iGuard is compatible with the DDNS service offered by Web Surveillance, LLC (www.websurveillance.com).

b. Port Forwarding

If you place the iGuard behind a router, you need to programme the router so that it can direct the specific incoming traffic to iGuard.

By default iGuard uses Port 80 for HTTP traffic (web manager) and port 9001 for video streaming. So you need forward port 80 traffic to the internal IP address of the iGuard.

If your Internet service Provider blocks port 80/9001 or you already host a website on the same network, you'll need to reconfigure your iGuard and router to other ports such as 81/9002, 82/9003, etc.

Note: The section you need to look for in the router is Port Forwarding or Virtual Server

C. Demilitarized Zone (DMZ)

iGuard uses port 9001 by default to stream video to the internet. Unfortunately this port is normally disabled or blocked by most commercial router's built-in firewall. In order for the iGuard applications to work properly, the firewall settings in the router need to be configured.

Some router has a very sophisticated built-in firewall. Instead of programming each port on the router, you can use the DMZ feature to by-pass the firewall setting.

Follow the steps below to configure your router. If your particular router manufacturer or model is not listed below, please contact your router manufacturer for further assistance in configuring the router.

The Following Router manufacturers and models are included in this document:

Brand	Model	Description
3Com	3C857-US	OfficeConnect Cable/DSL Gateway
	3CRWE52196	OfficeConnect Wireless Cable/DSL Gateway
Belkin	F5D6230-3	Wireless Cable/DSL Gateway Router
	F5D7230-4– 54g	Wireless DSL/Cable gateway Router
D-Link	DI-604/DI–614+/DI-624	-
	DI-704/704P	-
	DI714	-
	DI-714P+	-
Dell	TrueMobile 2300 Wireless Broadband Router	-
Linksys	BEFSR41	EtherFast Cable/DSL Router
	BEFSX41	Instant Broadband EtherFast Cable/DSL Firewall Router with 4-Port Switch/VPN EndPoint
	BEFW11S4	Wireless Access Point Router with 4-Port Switch – Version 2
Microsoft	MN-100	Wired Base Station
	MN-500	Wireless Base Station
NETGEAR	RP614	Web Safe Router
	MR814	Wireless Router
	MR314	Cable/DSL Wireless Router
	FVS318	ProSafe VPN Firewall
Proxim	ORiNOCO BG-2000 Broadband Gateway	-
Siemens	SpeedStream 2602	2-Port DSL/Cable Router
	SpeedStream 2623	Wireless DSL/Cable Router
	SpeedStream 2604	4-port DSL/Cable Router
	SpeedStream 2624	Wireless DSL/Cable Router
SMC	SMC2404WBR	Barricada Turbo 11/22 Mbps Wireless Cable/DSL Broadband Router
	SMC7004VBR	Barricada Cable/DSL Broadband Router
	SMC7004CWBR	Barricada Wireless Cable/DSL Broadband Router
	SMC7004AWBR	Barricade 4-port 11Mbps Wireless Broadband Router

3Com (http://www.3com.com)

3C857-US – OfficeConnect Cable/DSL Gateway
3CRWE52196 – OfficeConnect Wireless Cable/DSL Gateway

1. Log into your router using your router IP.

2. On the main page, select **Firewalls** on the left side of the page.

3. Select the **Virtual Servers** tab at the top of the page.

4. Click **New** on the right side of the page to open the Virtual Server Settings dialog box.

5. Type in the camera's IP address in the Server IP address text box.
6. Under Local Service, select **Custom**.

7. Under Custom Service Name, type in: **iGuard**.

8. Under Specify Custom Service Ports, type in: **80, 9001**.

9. Click **Add** to save the settings. The iGuard should now be configured to work with your router and be accessible from the internet.

Belkin (http://www.belkin.com)

F5D6230-3 – Wireless Cable/DSL Gateway Router

1. Log into your router using your router IP.

2. On the main page, select **Virtual Server** on the left side of the page under the Securit section.

3. Enter the following information on the page:

Line #1:

Private IP:	Type in the **camera's IP address**.
Private Port:	80
Type:	TCP
Public Port:	80

Line #2

Private IP:	Type in the **camera's IP address**.
Private Port:	9001
Type:	UDP
Public Port:	9001

4. Click **Enter** to save the settings. The iGuard should now be configured to work with your router and be accessible from the internet.

F5D7230-4 – 54g Wireless DSL/Cable gateway Router

1. Log into your router using your router IP.

2. On the main page, select **Firewall** on the left side of the page.

3. Under Firewall, select **Virtual Servers**.

4. Enter the following information on the page:

Line #1

Enable:	Checked in
Description:	iGuard - Webpage
Internet Port:	80 to 80
Type:	TCP
Private IP address:	Type in the **camera's IP address**.
Private Port	80 to 80

Line #2

Enable:	Checked in

Description:	iGuard – Camera
Internet Port:	9001 to 9001
Type:	UDP
Private IP address:	Type in the **camera's IP address**.
Private Port	9001 to 9001

5. Click **Apply Changes** to save the settings. The iGuard should now be configured o work with your router and be accessible from the internet.

D-Link (http://www.dlink.com)

DI-604/DI – 614+/DI-624

1. Log into your router using your router IP.

2. On the main page, click on **Advanced** at the top of the page.

3. On the left side of the page, click on **Virtual Server**. Note: Make sure DMZ host is disabled. If DMZ is enabled, it will disable all Virtual Server entries.

4. Enter the following information on the page:

Enable/Disable:	Enabled
Name:	iGuard - Webpage
Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5
Protocol Type:	TCP
Private Port:	80
Public Port:	80
Schedule:	Always

5. Click **Apply** to save the settings.

6. Enter the following information on the page:

Enable/Disable:	Enabled
Name:	iGuard - Webpage
Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5
Protocol Type:	UDP
Private Port:	9001
Public Port:	9001
Schedule:	Always

7. Click **Apply** o save the settings. iGuard should now be configured to work with your router and be accessible from the internet.

DI-704/704P

1. Log into your router using your router IP.

2. On the main page, click on **Advanced** at the top of the page.

3. On the **Virtual Server** page, enter the following information;

For ID#1:

Service Port:	80
Service IP:	Type in the **camera's IP address**, for example: 192.168.0.5

Enabled/Disabled: Enabled

For ID#2
Service Port: 9001
Service IP: Type in the **camera's IP address**, for example: 192.168.0.5
Enabled/Disabled: Enabled

4. Save your settings. iGuard should now be configured to work with your router and be accessible from the internet.

DI714

1. Log into your router using your router IP.

2. On the main page, click on **Advanced** at the top of the page.

3. Click on **Virtual Server Settings** on the left side of the page.

4. Enter the camera's IP address into the Internal IP field. Under Service, select **All** and then click **Submit** to save your settings. iGuard should now be configured to work with your router and be accessible from the internet.

DI-714P+

1. Log into your router using your router IP.

2. On the main page, click on **Advanced** at the top of the page.

3. On the left side of the page, click **Virtual Server**.

4. Enter the following information on the page:
For ID#1:
Service Port: 80
Service IP: Type in the **camera's IP address**, for example: 192.168.0.5
Enabled/Disabled: Enabled

For ID#2
Service Port: 9001
Service IP: Type in the **camera's IP address**, for example: 192.168.0.5
Enabled/Disabled: Enabled

5. Click **Apply** to save your settings. iGuard should now be configured to work with your router and be accessible from the internet.

Dell TrueMobile 2300 Wireless Broadband Router

(http://www.dell.com)

1. Log into your router using your router IP.

2. On the main page, click on **Advanced Settings** at the top of the page.

3. Go to the Port Forwarding and select Custom Port Forwarding Settings.

4. Check the **Enable** box.

5. Enter the desired name or description in the **Service Name** field such as **iGuard Web**.

6. In the **Incoming Ports** field, specify port **80** in both boxes.

7. In the **Destination IP Address** field, enter the IP address of iGuard

8. In the **Destination MAC Address** field, enter the MAC address of iGuard. You can find the camera's MAC address by either looking at the MAC address sticker on the bottom of the camera or by utilizing iGuard setup utility to display the MAC address.

Linksys (http://www.linksys.com)

BEFSR41 – EtherFast Cable/DSL Router

BEFSX41 – Instant Broadband EtherFast Cable/DSL Firewall Router with 4-Port Switch/VPN EndPoint

BEFW11S4 – Wireless Access Point Router with 4-Port Switch – Version 2

1. Log into your router using your router IP.

2. On the router's main page, click on **Advanced** at the top of the page.

3. On the next page, click on **Forwarding**.

4. Enter the following information on the page:

Line #1:

Customized Applications:	iGuard – Webpage
Ext. Port:	80 to 80
Protocol:	TCP
IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5
Enable:	Checked in

Line #2:

Customized Applications:	iGuard – Camera
Ext. Port:	9001 to 9001
Protocol:	UDP
IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5
Enable:	Checked in

5. Click on **Apply** to save the settings. iGuard should now be configured to work with your router and be accessible from the internet.

Microsoft (http://www.microsoft.com/hardware/broadbandnetworking)

MN-100 – Wired Base Station
MN-500 – Wireless Base Station

1. Log into your router using your router IP.

2. Open the Bass Station Management Tool, and then click **Security**.

3. On the Security menu, click **Port Forwarding**, and then click **Set up persistent port forwarding**.

4. In the Enable checkbox, check in the checkbox.

5. In the Description box, type a description of the server field such as: **iGuard Web**.

6. In the Inbound port boxes, type in: **80 – 80**. (i.e. from Port 80 to Port 80)

7. In the Type box, select the protocol as **TCP**.

8. In the Private IP address box, type in the **IP Address** of the iGuard network camera. For example, type in: 192.168.0.5.

9. In the Private port boxes, these values are automatically filled in from Step 6 and should already show **80 – 80**.

10. On the next empty line, repeat steps 4-9, except this time the Description should be **iGuard Cam** and the Inbound/Private port boxes should be **9001 – 9001** (UDP). The protocol and private IP address should be the same.

11. Click **Apply** to save the changes you have made. iGuard should now be configured to work with your router and be accessible from the internet.

NETGEAR (http://www.netgear.com)

RP614 – Web Safe Router
MR814 – Wireless Router

1. Log into your router using your router IP.

2. Click **Advanced -> Port Forwarding** on the left side of the page.

3. Click Add Customer Service.

4. Enter the following information on the page:

Service Name:	iGuard – Web
Starting Port:	80
Ending Port:	80
Server IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5

5. Click **Apply** to save the settings.

6. Enter the following information on the page:

Service Name:	iGuard – Cam
Starting Port:	9001
Ending Port:	9001
Server IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5

7. Click **Apply** to save the settings. iGuard should now be configured to work with your router and be accessible from the internet.

MR314 – Cable/DSL Wireless Router

1. Log into your router using your router IP.

2. Click **Advanced** on the left side of the page.

3. Click **Ports**.

4. Enter the following information on the page:

Line #1:

Starting Port:	80
Ending Port:	80
Server IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5

Line #2:

Starting Port:	9001
Ending Port:	9001
Server IP Address:	Type in the **camera's IP address**, for example: 192.168.0.5

5. Click **Apply** to save the settings. iGuard should now be configured to work with your router and be accessible from the internet.

FVS318 – ProSafe VPN Firewall

1. Log into your router using your router IP.

2. On the main page, click on **Add Service** on the left side of the screen.

3. Click Add Customer Service.

4. In the **Name** field enter a name for the camera, for example: **iGuard Web**:

Type:	TCP
Start Port:	81
Finish Port:	81

5. Click **Apply** to save the settings.

6. There is a bug in the NETGEAR FVS318 1.4 firmware that does not record any entry that uses port 80. If you intend to use port 80, you will initially need to enter 81 for the Start and Finish port, and then edit the entry to port back to 80. Click on **Add Service** on the left side of the screen.

7. In the **Service Table** window select iGuard Web and click **Edit Service**.

8. Change the **Start** and **Finish** port to **80**. Click **Apply**.

9. On the main page, click on **Add Service** on the left side of the screen and then click **Add Custom Service**. In the **Name** field enter a name for the camera, for example: **iGuard Cam**.

Type:	UDP
Start Port:	9001
Finish Port:	9001

10. Click **Apply** to save the settings.

11. On the main page, click on **Ports** at the side of the screen.
    A. Click **Add**.
    B. For Service Name select: iGuard Web
    C. Action: **ALLOW always**

D. Local Server Address: Enter the IP address of the camera
E. WAN Users Address: **Any**
F. Click **Apply**.

12. Click Add again.
A. For Service name select: **iGuard Cam**
B. Action: ALLOW always
C. Local Server Address: Enter the IP address of the camera
D. WAN Users Address: **Any**
E. Click **Apply**.

13. Exit the router setup program. iGuard should now be configured to work with your router and be accessible from the internet.

Proxim (http://www.proxim.com)

ORiNOCO BG-2000 Broadband Gateway

1. Log into your router using your router IP.

2. On the router's main page, click on **Setup** at the top of the page.

3. On the left side of the page, click on **Advanced settings -> Port Forwarding**.

4. Check in the checkbox for **Enable Port Forwarding**.

5. Click **New** on the right side of the page.

6. Enter the following information on the page:

Global Port:	80
Local Address:	Type in the **camera's IP address**, for example: 192.168.0.5
Local Port:	80
Type:	TCP

7. Click **Save** to save the settings.

8. Click **New** on the right side of the page.

9. Enter the following information on the page.

Global Port:	9001
Local Address:	Type in the **camera's IP address**, for example: 192.168.0.5
Local Port:	9001
Type:	UDP

10. Click **Save** to save the settings.

11. Click **Restart** on the left side of the page to restart your router. iGuard should now be configured to work with your router and be accessible from the internet.

Siemens (http://www.speedstream.com)

SpeedStream 2602 – 2-Port DSL/Cable Router
SpeedStream 2623 – Wireless DSL/Cable Router
SpeedStream 2624 – Wireless DSL/Cable Router

1. Log into your router using your router IP.

2. After you are logged in, click on **Advanced Setup -> Virtual Servers**.

3. Enter the following information on the page:

Line #1:	
Private IP:	Type in the **camera's IP address**,
Private Port:	80
Type:	TCP
Public Port:	80
Line #2	
Private IP:	Type in the **camera's IP address**,
Private Port:	9001
Type:	UDP
Public Port:	9001

4. Click **Enter** to save the settings. iGuard should now be configured to work with your router and be accessible from the internet.

SpeedStream 2604 – 4-port DSL/Cable Router

1. Log into your router using your router IP.

2. After you are logged in, click on **Advanced Setup -> Virtual Servers**.

3. Under the Properties section, there are a few entries you'll need to add. Check in the checkbox for **Enable**.

4. Under the first box, next to the Enable checkbox, type in: **iGuard Web**.

5. Under PC (Server), select your camera or the camera's IP address from the list. If the camera is not listed, select the link titled "My PC is not listed."

6. Leave Protocol as **TCP**.

7. Under Internal Port No type in: **80**

8. Under External Port No type in: **80**

9. Click on **Add** to save these settings.

10. Under the first box, next to the Enable checkbox, type in: **iGuard Cam**.

11. Under PC (Server), select your camera or the camera's IP address from the list. If the camera is not listed, select the link titled "My PC is not listed."

12. Leave Protocol as **TCP**.

13. Under Internal Port No type in: **9001**

14. Under External Port No type in: **9001**

15. Click on **Add** to save these settings. iGuard should now be configured to work with your router and be accessible from the Internet.

SMC (http://www.smc.com)

SMC2404WBR – Barricada Turbo 11/22 Mbps Wireless Cable/DSL Broadband Router
SMC7004VBR – Barricada Cable/DSL Broadband Router
SMC7004CWBR – Barricada Wireless Cable/DSL Broadband Router

1. Log into your router using your router IP.

2. After you are logged in, click **NAT** on the left side of the page.

3. Click on **Virtual Server** on the left side of the page.

4. Enter the following information on the page:

Line #1:

Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5
Private Port:	80
Type:	TCP
Public Port:	80

Line #2

Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5
Private Port:	9001
Type:	UDP
Public Port:	9001

5. Click **Apply** to save the settings. iGuard should now be configured to work with your router and be accessible from the Internet.

SMC7004AWBR – Barricade 4-port 11Mbps Wireless Broadband Router

1. Log into your router using your router IP.

2. Click on **Virtual Server** on the left side of the page.

3. Enter the following information on the page:

For ID #1:

Service Port:	80
Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5
Enable:	Checked in

For ID #2:

Service Port:	9001
Private IP:	Type in the **camera's IP address**, for example: 192.168.0.5
Enable:	Checked in

4. Click **Save** to save the settings. iGuard should now be configured to work with your router and be accessible from the Intern

Appendix B: IP Address, Subnet and Gateway

This section discusses Communities, Gateways, IP Addresses and Subnet masking

Communities
A community is a string of printable ASCII characters that identifies a user group with the same access privileges. For example, a common community name is "public." For security purposes, the SNMP agent validates requests before responding. The agent can be configured so that only trap managers that are members of a community can send requests and receive responses from a particular community. This prevents unauthorized managers from viewing or changing the configuration of a device.

Gateways
Gateway, also referred to as a router, is any computer with two or more network adapters connecting to different physical networks. Gateways allow for transmission of IP packets among networks on an Internet.

IP Addresses
Every device on an Internet must be assigned a unique IP (Internet Protocol) address. An IP address is a 32-bit value comprised of a network ID and a host ID. The network ID identifies the logical network to which a particular device belongs. The host ID identifies the particular device within the logical network. IP addresses distinguish devices on an Internet from one another so that IP packets are properly transmitted.

IP addresses appear in dotted decimal (rather than in binary) notation. Dotted decimal notation divides the 32-bit value into four 8-bit groups, or octets, and separates each octet with a period. For example, 199.217.132.1 is an IP address in dotted decimal notation.

To accommodate networks of different sizes, the IP address has three divisions – Classes A for large, B for medium and C for small. The difference among the network classes is the number of octets reserved for the network ID and the number of octets reserved for the host ID.

Class	Value of First Octet	Network ID	Host ID	Number of Hosts
A	1-126	First octet	Last three octets	16,387,064
B	128-191	First two octets	Last two octets	64,516
C	192-223	First tree octets	Last octet	254

Any value between 0 and 255 is valid as a host ID octet except for those values the InterNIC reserves for other purposes

Value	Purpose
0, 255	Subnet masking
127	Loopback testing and interprocess communication on local devices
224-254	IGMP multicast and other special protocols.

Subnetting and Subnet Masks
Subnetting divides a network address into sub-network addresses to accommodate more than one physical network on a logical network.

For example:
A Class B company has 100 LANs (Local Area Networks) with 100 to 200 nodes on each LAN. To classify the nodes by its LANs on one main network, this company segments the network address into 100 sub-network addresses. If the Class B network address is 150.1.x.x, the address can be segmented further from 150.1.1.x through 150.1.100.x

A subnet mask is a 32-bit value that distinguishes the network ID from the host ID for different sub-networks on the same logical network. Like IP addresses, subnet masks consist of four octets in dotted decimal notation. You can use subnet masks to route and filter the transmission of IP packets among your sub-networks. The value “255” is assigned to octets that belong to the network ID, and the value “0” is assigned to octets that belong to the host ID.

For the example above, if you want all the devices on the sub-networks to receive each other’s IP packets, set the subnet mask to 255.255.0.0. If you want the devices on a single sub-network only to receive IP packets from other devices on its own sub-network, set the subnet mask to 255.255.255.0 for the devices on the sub-network.

Subnet Mask	Routing and Filtering
0.0.0.0	IP packets are transmitted to all devices.
255.0.0.0	IP packets are only transmitted to devices that are IP that’s first octet matches the sender’s IP address’s first octet.
255.255.0.0	IP packets are only transmitted to devices that are IP that’s first two octets match the sender’s IP address’s first two octets.
255.255.255.0	IP packets are only transmitted to devices that are IP that’s first three octets match the sender’s IP address’s first three octets.

Appendix C: Glossary

The Glossary defines the terms used in this User Manual

Term	Definition
Ethernet	Local Area Network technology, originally developed by Xerox Corporation, can link up to 1,024 nodes in a bus network. Ethernet provides raw data transfer in a rate of 10 megabits/sec. with actual throughputs in 2 to 3 megabits/sec. using a baseband (single-channel) communication technique. Ethernet uses carrier sense multiple access collision detection (CSMA/CD) that prevents network failures when two devices attempt to access the network at the same time. LAN hardware manufacturers use Ethernet protocol; their products may not be compatible.
Gateway	A computer that attaches to a number of networks and routes packets between them. The packets can be different protocols at the higher levels.
IP	Internet Protocol – The TCP/IP standard protocol defines the IP datagram as the unit of information passed across a network.
IP Address	Internet Protocol Address – A 32-bit address assigned to hosts participating in a TCP/IP network. The IP address consists of network and host portions. It is assigned to an interconnection of a host to a physical network.
MAC	Medium Access Control - The network layer between the physical and the data link layers. Specifically, the physical (hardware) address exists in this layer.
MIB	Management Information Base – The database, i.e. set of variables maintained by a gateway running SNMP
NMS	Network Management Station
OID	Object Identifier – The variables defined in a MIB
Router	A computer that manages traffic between different network segments or different network topologies. It directs the destination IP address. The network media can be different, but the higher-level protocols must be the same.
SNMP	Simple Network Management Protocol – A standard protocol used to monitor IP hosts, networks, and gateways. SNMP defines a set of simple operations that can be performed on the OIDs of the MIBs managed by the monitored Agents. It employs the UDP/IP transport layer to move its object between the Agents and the NMS
TCP/IP	Transmission Control Protocol/ Internet Protocol – A protocol suite used by more than 15 million users with a UNIX association and widely used to link computers of different kinds.

Appendix D: Q&A

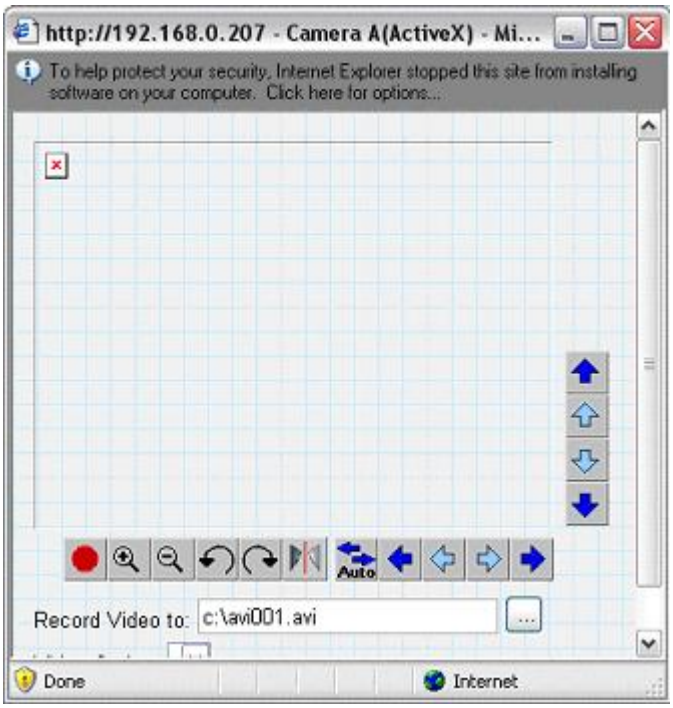
Q1. I have set a permission level without first setting an "Administrator" first and now I can't change anything.

You will need to update the firmware. Download the firmware and use *iGuard Utility* to upload it into iGuard. Once completed, the Username and Passwords will be reset to default. Always remember to save your iGuard configuration for use later.

Q2. Can I use other USB Camera to connect to iGuard?

Yes, provided that the camera is using VIMICRO chip. You will have to check with the manufacturer of the USB camera. Currently, about 60% to 70% of the cameras produced in China uses this chip.

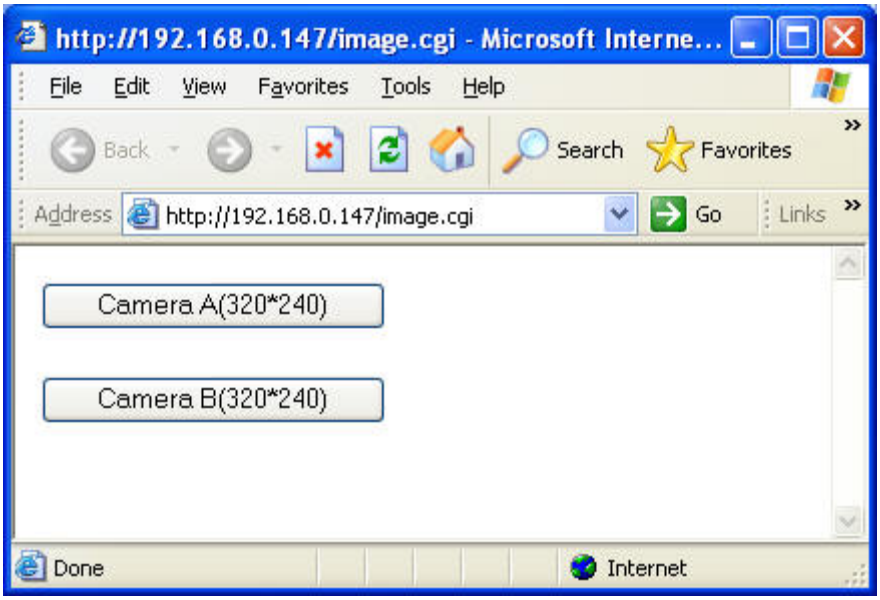
Q3. I get the following message, when I click on ActiveX



Click on the top margin, and install ActiveX. Also make sure that you have firmware v2.37, if not you'll need to upgrade.

Q4. How can I view images from my web enabled PDA?

Please make sure that you have a GRPS enabled PDA. Use the browser and type in **http://xxx.xxx.xxx.xxx/image.cgi** (where xxx is the WAN IP address or your Domain Name). You will then be directed to this page;



Click on either "Camera A (320*240)" or "Camera B (320*240)" to view the image.

Click "Refresh" to download the next image. Click "Back" to go back to the above page.

Q5. What is the effective length of the USB cable?

The industrial Standard for effective USB cable length is 5.0m from source to source. If you so decide to extend the length, you can purchase a USB extension

Q6. What is the effective length of the RJ-45 cable?

The Standard effective length per RJ-45 cable is 100m, you will need a hub per 100m extension, up to a maximum of 480m.

Q7. Can I use iGuard outdoors?

iGuard is designed primarily for indoor use. For outdoor use you will need a protective housing. This is not supplied.

Q8. Is the camera capable of zooming by adding a zoom lens?

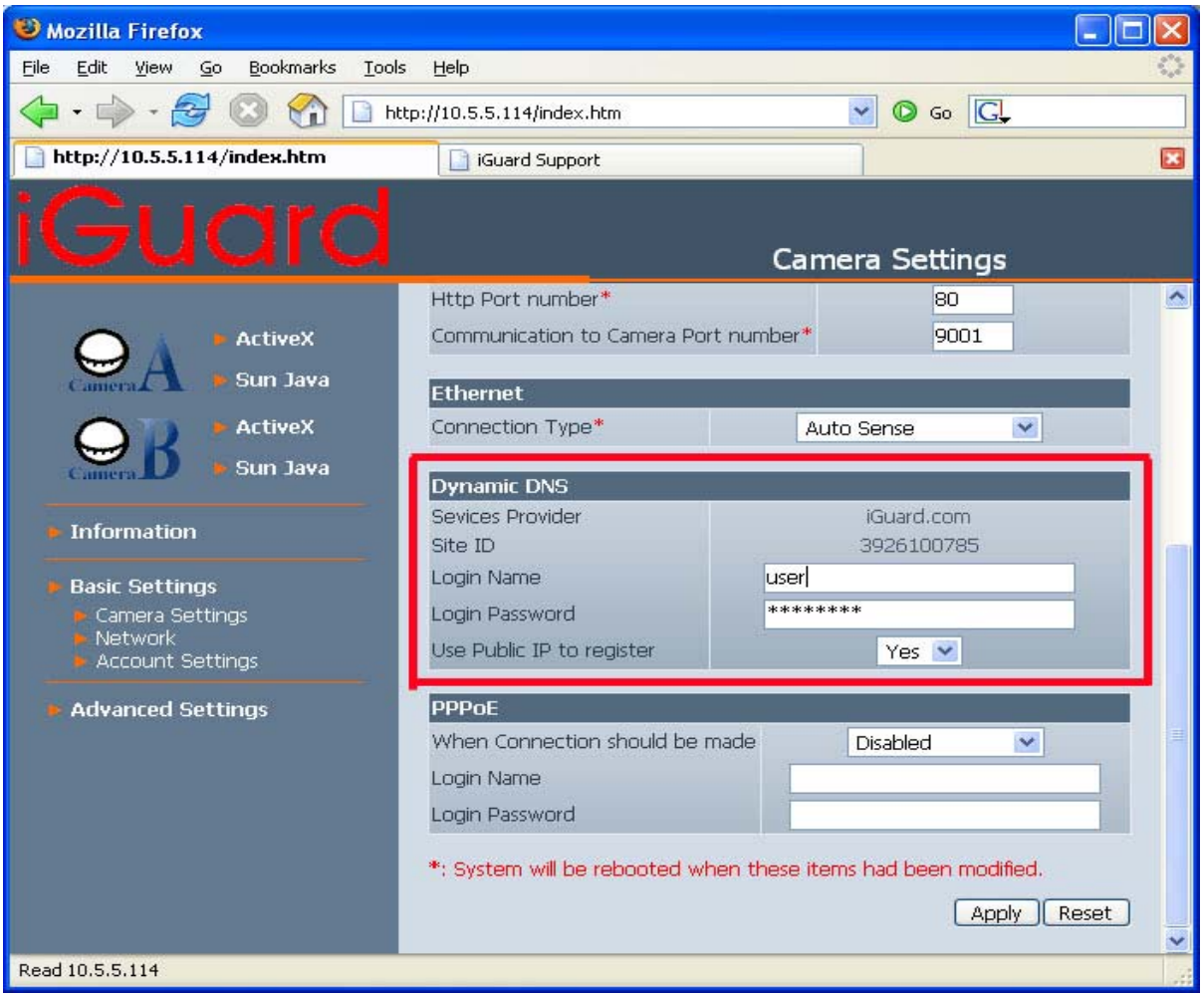
You can add a zoom lens, but will have to adjust the zoom manually. The default camera does not support 'remote' zoom.

Q9. My iGuard is connected to a Router and I can see it in LAN but my friends can't see it from the Web? How do I set up iGuard for the web?

For users with DYNAMIC IP;

(a) Contact iGuard.com Customer Support for a DDNS account (self-registration coming soon) and register your iGuard cameras

(b) From your PC log-on to your iGuard as Administrator. Enter your username and password for your iGuard.com account. Make sure the "Use Public IP to Register" is set to "Yes" Then Click "Apply" located at the bottom of screen.



Note: Please allow 5 minutes for the DDNS server to be updated with your Current WAN IP.

If iGuard is connected to a Router or IP Share then;

(d) Go to your Address Translation / NAT / Firewall section of your ROUTER. Open up TCP port 80 and UDP port 9001, make sure that the TCP port is not currently used by your router, otherwise choose a different port.

Note: Here you are using iGuard to check your current WAN IP and update the DDNS server. Alternatively, if your ROUTER supports DDNS, you can input the above details (b) in your ROUTER. In which case, your ROUTER will update the DDNS server with your current WAN IP.

If iGuardView is connected to your xDSL line or HUB, then;

(e) In iGuard, goto Basic Settings --> Network --> PPPoE, and enter the details.

For users with STATIC IP; proceed directly to (d) or (e).

Q10. I'm connecting iGuard to a HUB, how do I set it to access the internet?

1. Make sure that PPPoE section in iGuard is setup to connect to your ISP, and;

2. Make sure that Dynamic DNS in iGuard is setup.

Q11. I can not access iGuard Web Manager. I have opened up all the ports.

1. Check that your Router and iGuard are not both also using EXTERNAL / WAN port 80. If it is, change one to another EXTERNAL / WAN port.

2. If you changed iGuard default HTTP port 80 to another say, port 8081. Then you will have to redirect your web browser by typing **http://xxx.xxx.xxx.xxx:8081** where http://xxx.xxx.xxx.xxx is iGuard IP address.

Q12. I can access iGuard Web Manager but cannot view images when clicking ActiveX / SunJava.

Make sure that you have a UDP port 9001 opened.

Q13. There is no Port Forwarding Section in my Router.

Different Routers have different setup for this section. In general, a more advanced router will allow you to forward *Internal / LAN* port to an *External / WAN* port. You can assign an internal port number to be forwarded to a different external port number.

However, there are also Routers which can not do this. Your internal port = external port, and you are only allowed to open a *range* of ports. Please check with your router's manufacturer on how to open the port for your router.

Q14. I setup the Email Server (SMTP) but I can't seem to receive any emails.

Make sure that your Internet Security Software / SPAM software does not block outgoing emails.

Q15. What bandwidth is required by iGuard?

The average "Bytes of Image per Frame" is between 4Kbytes - 9Kbytes. This size is determined according to color saturation of the image captured. Therefore, the "Frame per Second" (FPS) = "Data transmission rate" (in Bytes/s) divided by "Bytes of Image per Frame" (Bytes/frame)

You can check your current FPS setting in iGuard. Network --> Account Settings --> FPS (default is 10)

At 10 FPS, iGuard will need about 40Kbytes - 90Kbytes of bandwidth.

NOTE:

bps = bits per second (8 bits =1 Byte)

Most ADSL throughput speed varies, and is dependent on distance and environmental constraints. In most cases the actual throughput is only about 75%.

If you are using 56Kbps dial-up, your average speed should be around 4 Kbytes/sec - 6 Kbytes/sec

If you are using 512Kbps ADSL, your average speed should be around 40 Kbytes/sec - 50 Kbytes/sec If you are using T1 (1536Kbps) ADSL, your average speed should be 120 Kbytes/sec or higher.

If you are using 2M (2000Kbps) ADSL, your average speed should be 160 Kbytes/sec or higher.